



# Installation Guide

for use with

**Check Point® FireWall-1®**

Websense Enterprise®

Websense® Web Security Suite™



**v6.3.3**

©1996–2009, Websense, Inc.  
10240 Sorrento Valley Rd., San Diego, CA 92121, USA  
All rights reserved.

Published February 19, 2009  
Printed in the United States of America and Ireland

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 6,606,659 and 6,947,985 and other patents pending.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Websense, Inc.

Every effort has been made to ensure the accuracy of this manual. However, Websense, Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense, Inc., shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

## **Trademarks**

Websense and Websense Enterprise are registered trademarks of Websense, Inc., in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Check Point, OPSEC, FireWall-1, VPN-1, SmartDashboard, and SmartCenter are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates.

Microsoft, Windows, Windows NT, Windows Server, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Sun, Solaris, UltraSPARC, Sun Java System, and all Sun Java System based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc., in the United States and other countries.

Red Hat is a registered trademark of Red Hat, Inc., in the United States and other countries. Linux is a trademark of Linus Torvalds in the United States and other countries.

Novell, Novell Directory Services, eDirectory, and ZENworks are trademarks or registered trademarks of Novell, Inc., in the United States and other countries.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the U.S. and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

This product includes software developed by the Apache Software Foundation ([www.apache.org](http://www.apache.org)).  
Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

## **WinPcap**

Copyright (c) 1999 - 2009 NetGroup, Politecnico di Torino (Italy).  
Copyright (c) 2009 CACE Technologies, Davis (California).  
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Politecnico di Torino, CACE Technologies nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

# Contents

<b>Chapter 1</b>	<b>Introduction</b> .....	<b>7</b>
	About this Guide .....	7
	Document Conventions .....	8
	Where to Find More Information .....	8
	Websense Components .....	8
	How Websense Filtering Works .....	11
	Steps for a Successful Websense Deployment .....	12
<b>Chapter 2</b>	<b>Network Configuration</b> .....	<b>15</b>
	Websense Enterprise/Web Security Suite Components .....	15
	Deploying Websense Components with your Integration Product .....	24
	Simple .....	24
	Distributed .....	25
	Websense Reporting Components .....	27
	Directory Services .....	27
	Filtering in a Network with Citrix® Server Users .....	30
	System Requirements .....	30
	Supported Check Point FireWall-1 Versions .....	31
	User Workstations .....	31
<b>Chapter 3</b>	<b>Upgrading Websense Enterprise/Web Security Suite</b> .....	<b>33</b>
	Versions Supported .....	34
	Transferring Configuration Data Without Upgrading .....	35
	Before You Upgrade .....	36
	Upgrading on Windows .....	38
	Upgrading on Solaris or Linux .....	45
	Upgrading the Remote Filtering Components .....	50
	Remote Filtering Server .....	50

	Remote Filtering Client Pack . . . . .	50
	Remote Filtering Client . . . . .	50
	Converting a Stand-Alone System to an Integrated System . . . . .	54
	All Websense Filtering Components on the Same Machine. . . . .	55
	Distribute Websense Filtering Components . . . . .	55
	Upgrading to the New Stand-Alone Edition . . . . .	57
	Converting to an Integrated System . . . . .	66
	Updating the Websense Resource Object . . . . .	71
	Migrating Between FireWall-1 Versions After an Upgrade . . . . .	71
	Changing IP Addresses of Installed Components . . . . .	72
<b>Chapter 4</b>	<b>Installing Websense Enterprise/Websense Web Security Suite . . . .</b>	<b>73</b>
	Websense Installers . . . . .	73
	Non-English Language Versions . . . . .	73
	Before Installing . . . . .	75
	Typical Websense Installation . . . . .	78
	Windows . . . . .	78
	Solaris or Linux . . . . .	91
	Installing Websense Components Separately . . . . .	101
	Windows Procedures . . . . .	103
	Solaris and Linux Procedures . . . . .	143
	Modifying an Installation . . . . .	163
	Adding Components . . . . .	163
	Removing Components . . . . .	173
	Repairing an Installation . . . . .	178
	Repairing the Policy Server . . . . .	183
	Migrating between FireWall-1 Versions After Installation . . . . .	185
	Stopping or Starting Websense Services . . . . .	185
	Manually Stopping Services . . . . .	185
	UFP Server . . . . .	186
	Windows . . . . .	186
	Solaris and Linux . . . . .	188
<b>Chapter 5</b>	<b>Initial Setup . . . . .</b>	<b>189</b>

---

Subscription Key and Master Database Download . . . . .	190
Identifying the Filtering Service for the Block Page URL . . . . .	194
Displaying Protocol Block Messages . . . . .	195
Creating and Running the Script for Logon Agent . . . . .	196
Prerequisites for Running the Logon Script . . . . .	196
File Location. . . . .	197
Deployment Tasks . . . . .	197
Preparing the Logon Script. . . . .	198
Configuring the Logon Script to Run. . . . .	201
Configuring Network Agent to use Multiple NICs . . . . .	204
Testing Visibility of Internet Traffic to Network Agent . . . . .	204
Running the Websense Traffic Visibility Tool . . . . .	204
Configure Domain Administrator Privileges. . . . .	207
User Service and DC Agent on Windows . . . . .	207
DC Agent on Linux . . . . .	207
Activating the Websense Web Protection Services™. . . . .	208
SiteWatcher™ . . . . .	208
BrandWatcher™. . . . .	208
ThreatWatcher™ . . . . .	209
Firewall Configuration for Remote Filtering. . . . .	209
Enabling communication between Remote Filtering Server and Remote User Workstations. . . . .	209
Enabling communication between Remote Filtering Server and Filtering Service . . . . .	210
Blocking remote users' internet access when Remote Filtering is unavailable. . . . .	210
Configuring the Remote Filtering Client Log . . . . .	212
<b>Chapter 6 Using FireWall-1 with Websense Software . . . . .</b>	<b>215</b>
Distributed FireWall-1 Environments . . . . .	217
Client Workstations and FireWall-1 . . . . .	217
Communicating with Websense Software. . . . .	217
Enhanced UFP Performance . . . . .	218
Caching . . . . .	219
Strategy. . . . .	219

	Options .....	220
<b>Chapter 7</b>	<b>Configuring FireWall-1 NG, NG with AI, and NGX.....</b>	<b>223</b>
	Creating an OPSEC Application Object .....	224
	Creating Resource Objects.....	228
	Defining Rules .....	231
	Establishing Secure Internal Communication (SIC) .....	234
	Prerequisites .....	234
	Configuring FireWall-1 to Use SIC .....	235
	Configuring the Websense Software to Use SIC .....	237
	Updating the OPSEC Application Object.....	239
	Restoring Clear Communication .....	242
	Enhanced UFP Performance .....	245
	Websense Configuration.....	245
	FireWall-1 Configuration .....	246
<b>Appendix A</b>	<b>Stealth Mode.....</b>	<b>251</b>
	Configuring for Stealth Mode .....	251
	Windows .....	252
	Solaris or Linux.....	253
<b>Appendix B</b>	<b>Troubleshooting .....</b>	<b>255</b>
<b>Appendix C</b>	<b>Technical Support .....</b>	<b>275</b>
	Online Help .....	275
	Technical Support.....	275
<b>Index.....</b>		<b>279</b>

Thank you for choosing Websense® web filtering and web security software. This guide covers installation and initial setup of Websense Enterprise® or Websense® Web Security Suite™ integrated with Check Point® FireWall-1®.

Websense, Inc., strongly recommends that your users be informed of your organization's policies concerning internet access, and that Websense software has been installed as a tool for monitoring activity and/or enforcing your internet use policies.

## About this Guide

---

This guide can be used with the following Websense products:

- ◆ Websense Enterprise®
- ◆ Websense® Web Security Suite™

The installation and initial setup information provided in this guide applies to the *web filtering* components of these products.

For additional information about the web filtering components in the Websense Enterprise/Web Security Suite products:

- ◆ See the *Deployment Guide* for Websense Enterprise/Web Security Suite before installing the web filtering components to learn how to deploy these components in your network.
- ◆ See the *Administrator's Guide* for Websense Enterprise/Web Security Suite after installing the web filtering components for information about configuring and customizing web filtering and web security features.

The rest of the components available in the Websense Enterprise/Web Security Suite products are documented as follows:

- ◆ *Reporting Tools for web filtering* (available in all Websense products listed above): For information about installing, configuring, and using these web filtering reporting components, see the Websense Reporting documentation set. For information about planning deployment of web

filtering reporting components in your network prior to installation, see the *Deployment Guide* for Websense Enterprise/Web Security Suite.

- ◆ *Desktop filtering* and *desktop filtering reporting* is available with Websense Client Policy Manager™ (CPM). For information about installing, configuring, and using desktop filtering and desktop filtering reporting, see the CPM documentation set.

## Document Conventions

References to “Websense software” in this guide apply to Websense Enterprise/Web Security Suite, unless specifically stated otherwise.

## Where to Find More Information

Websense product documentation, including all documents referenced in this guide, is available on the Websense website at:

[www.websense.com/docs/](http://www.websense.com/docs/)

## Websense Components

---

The following list provides an overview of the Websense Enterprise/Web Security Suite web filtering components, and includes brief descriptions of the Reporting Tools for web filtering.

- ◆ **Policy Server:** Stores all Websense configuration information, including filtering policies, and communicates this data to other Websense services.
- ◆ **Filtering Service:** Interacts with Check Point FireWall-1 and Network Agent to filter internet requests. Filtering Service either permits the internet request or sends an appropriate block message to the user.
- ◆ **Websense Manager:** Administrative interface that allows you to configure and manage Websense functionality through the Policy Server. Websense Manager is used to define and customize internet access policies, add or remove clients, configure Policy Server, and much more.
- ◆ **User Service:** Communicates with directory services in your network to allow you to apply filtering policies based on users, groups, domains, and organizational units.
- ◆ **Network Agent:** Manages the internet protocols that are not managed by Check Point FireWall-1. Detects HTTP network activity and instructs the



Filtering Service to log this information. You must install Network Agent and configure it properly to use the Bandwidth Optimizer, Protocol Management, and IM Attachment Manager features, and to log the number of bytes transferred and duration of transfer. Network Agent is also used to manage HTTP, HTTPS, and FTP filtering for a Stand-Alone (non-integrated) Websense installation.

- ◆ **Usage Monitor:** Tracks users' internet activity and sends alerts to Websense administrators when configured threshold values are crossed.
- ◆ **DC Agent:** An optional component that transparently identifies users who authenticate through a Windows® directory service. DC Agent enables filtering of internet requests according to policies assigned to particular users or groups.
- ◆ **RADIUS Agent:** An optional component that works through a RADIUS Server to transparently identify users and groups who access your network using a dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), or other remote connections.
- ◆ **eDirectory Agent:** An optional component that works together with Novell® eDirectory™ to transparently identify users so that Websense can filter them according to particular policies assigned to users or groups.
- ◆ **Logon Agent:** An optional component that works with a Websense client application (`LogonApp.exe`) to transparently identify users as they log on to a Windows domain via client machines. Logon Agent can be used with a Windows NT®-based directory service or with Active Directory®, which is LDAP-based. Logon Agent receives its user information from the logon application, `LogonApp.exe`, which must be run by a logon script in your network.
- ◆ **Real-Time Analyzer™ (RTA):** Displays the real-time status of all the traffic filtered by Websense Enterprise/Web Security Suite. RTA graphically displays bandwidth information and shows requests by category or protocol.
- ◆ **Remote Filtering Server:** An optional component that provides web filtering for machines located outside your organization's network firewall or internet gateway. In order to be filtered through the Remote Filtering Server, a remote workstation must be running the Remote Filtering Client. The Remote Filtering Server is enabled only if you subscribe to the remote filtering service.

- ◆ **Remote Filtering Client:** An optional component installed on client machines, such as notebook computers, that will be used outside your organization's network firewall or internet gateway. This component connects with a Remote Filtering Server inside the network firewall to enable web filtering of the remote workstation. The Remote Filtering Client is enabled only if you subscribe to the Remote Filtering service.



**Note**

The Remote Filtering Client is also available as part of the Client Agent in the Websense Client Policy Manager™ (CPM). For more information, see your Websense Client Policy Manager documentation.

---

- ◆ **Websense Master Database:** Contains a collection of millions of internet sites, each categorized by content. In addition, the Master Database contains protocols for such things as streaming media, peer-to-peer file sharing, and instant messaging.
- ◆ **Websense Enterprise Reporter:** This reporting tool is available free of charge with your Websense Enterprise/Web Security Suite subscription. Its Log Server component records internet activity on your network. Using this log information, Reporter can generate a wide variety of reports and charts depicting your network's internet usage trends. These reports can be used to refine internet filtering strategies, helping to maximize network resources and employee productivity. For installation procedures, see the *Reporting Installation Guide* for Websense Enterprise/Web Security Suite.
- ◆ **Websense Enterprise Explorer:** This reporting tool is available free of charge with your Websense Enterprise/Web Security Suite subscription. Explorer is a web-based reporting application that provides a customizable view into the Log Database. It displays summary information, as well as specific detail about users' internet activity. For installation procedures, see the *Reporting Installation Guide* for Websense Enterprise/Web Security Suite.
- ◆ **Websense Enterprise Explorer for Unix:** This reporting tool is available free of charge with your Websense Enterprise/Web Security Suite subscription. It is provided in a separate installer from the rest of the Websense Enterprise/Web Security Suite components. Explorer for Unix is a web-based reporting application that provides the same functionality as Websense Enterprise Explorer, but for Solaris and Linux operating

systems. For installation procedures, see the *Explorer for Unix Administrator's Guide* for Websense Enterprise/Web Security Suite.

## How Websense Filtering Works

---

The Websense Filtering Service is the engine by which internet content filtering is enforced. With its flexible, policy-based filtering approach, Websense software allows you to apply different filtering policies to different clients (users, groups, domains/organizational units, workstations, or networks).

When Check Point FireWall-1 receives an internet request from a client, it queries the Websense Filtering Service to find out whether the requested site should be blocked or not. To make this determination, Filtering Service consults the policy assigned to the client. Each policy delineates specific time periods during the week and lists the category sets that are in effect during those time periods. After it determines which categories are blocked, Filtering Service consults its comprehensive database of internet addresses (URLs). If the site is assigned to a blocked category, the user receives a block page instead of the requested site. If the site is assigned to a permitted category, Filtering Service notifies Check Point FireWall-1 that the site is not blocked, and the site is returned to the user.

Websense Enterprise/Web Security Suite filter network applications that use TCP-based protocols and measure bandwidth usage of UDP-based messages as well. If an initial internet request is made with TCP, and the request is blocked by the Websense software, all subsequent UDP traffic will also be blocked. UDP protocols such as RTSP and RTP are monitored and logged.

The Quota feature is an alternative to full blocking. It gives employees time each day to visit sites in categories you deem appropriate. Quotas can be a powerful tool for internet access management. Quotas help you control how much time your employees spend on personal surfing and the types of sites they are able to access. For more information, see the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

The Protocol Management feature allows Websense software to filter internet protocols other than HTTP. This includes protocols, applications, or other data transfer methods such as those used for instant messaging, streaming media, file sharing, file transfer, internet mail, and various other network or database operations. You must install Network Agent to use protocol management.

If you have a subscription that includes the Bandwidth Optimizer module and have installed Network Agent, your Websense software can filter internet sites, protocols, or applications based on available network bandwidth. You can specify filtering settings to limit user access to sites, protocols, or applications based on bandwidth usage.

If you have a subscription that includes the Instant Messaging (IM) Attachment Manager and have installed Network Agent, you can configure your Websense software to restrict file attachment sending and file sharing with IM clients. This feature enhances the default IM controls in Websense Enterprise/Web Security Suite by allowing you to permit certain IM traffic while blocking the transfer of attachments by those IM clients.

## Steps for a Successful Websense Deployment

---

The following sequence is recommended for installing Websense Enterprise or Web Security Suite and configuring it to filter internet traffic in conjunction with Check Point FireWall-1.

1. **Plan the Websense deployment:** Websense components can be deployed in various combinations, depending upon the size and architecture of your network. Deciding which Websense components to install and where to put them is your first task. The information required to make this decision can be found in the *Deployment Guide* for Websense Enterprise/Web Security Suite. For an overview of basic deployment in a small network (< 500 users), and deployment information specific to your integration product, see [Chapter 2: Network Configuration](#).
2. **Install Websense filtering components:** Once you have decided how to deploy Websense software in your network, install the selected web filtering components. See [Chapter 4: Installing Websense Enterprise/Websense Web Security Suite](#) for installation procedures.
3. **Perform initial setup tasks:** Perform the post-installation setup tasks in [Chapter 5: Initial Setup](#).
4. **Configure FireWall-1:** Configure your version of FireWall-1 to communicate with Websense software. For instructions, see [Chapter 6: Using FireWall-1 with Websense Software](#) and [Chapter 7: Configuring FireWall-1 NG, NG with AI, and NGX](#).

5. Once you have completed the previous tasks to set up default global web filtering, you can customize your filtering policies, configure user- and group-based filtering, and learn to use more advanced Websense features by following the instructions in the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

After the Websense filtering components have been successfully installed, install and configure the web filtering reporting components (Reporting Tools) so you can analyze and report on internet usage in your network. Use the information in the reports to tailor filtering policies for your organization. See the Websense Reporting documentation for instructions.



Websense components can be installed in a number of possible configurations, depending upon the nature of your network and your filtering requirements. To determine the appropriate deployment for your network, and for a complete list of system requirements, see the *Deployment Guide* for Websense Enterprise/Web Security Suite.

The information in this chapter provides an overview of where Websense components can be installed, with specific information about where to install Websense components in relation to your integration product.

## Websense Enterprise/Web Security Suite Components

When deciding how to deploy Websense Enterprise/Web Security Suite components in your network, consider the following installation dependencies:

- ◆ **Filtering Service:** Typically installed on the same machine as Policy Server and may be installed on the same machine as Websense Manager. The Filtering Service can be installed on a different operating system than the Policy Server, as long as they are properly configured to communicate with each other. This is an unusual deployment. Filtering Service installs on Windows, Solaris™, and Linux®. You can install a maximum of 10 Filtering Services for each Policy Server if they employ quality network connections. For additional information, see the *Deployment Guide* for Websense Enterprise/Web Security Suite.
- ◆ **Policy Server:** Typically installed on the same machine as the Filtering Service, but may be installed on a separate machine, depending upon the configuration of your network. There must be only one Policy Server installed for each *logical* installation. An example would be a Policy Server that delivers the same policies and categories to each machine in a subnet. The Policy Server installs on Windows, Solaris, and Linux.
- ◆ **Websense Manager:** May be installed on the same machine as Policy Server, and/or on one or more different machines in your network.

Websense Manager machine needs network access to the Policy Server machine, but the two machines do not need to have the same operating system. Websense Manager installs on Windows, Solaris, and Linux.

- ◆ **User Service:** Installed in networks using a directory service for authentication. User Service is unnecessary if you intend to filter and log internet requests based on client workstation IP addresses only. User Service can be installed on the same operating systems supported by the Policy Server and is typically installed on the same machine; however, you may install User Service on a different operating system than the Policy Server. If the Policy Server is installed on Linux, for example, you can install User Service separately on a Windows machine. User Service installs on Windows, Solaris, and Linux.



### Important

You can have only one User Service installation for each Policy Server in your network.

---

For systems providing multilingual support, User Service produces correct results for one *locale* only. The locale of the Policy Server determines the language it supports for directory services. Organizations with multilingual support requirements must install the product suite (User Service, Policy Server, and Filtering Service) for each supported language on machines configured for that language.

- ◆ **Network Agent:** Can be installed on the Filtering Service machine or separately, depending upon your needs and the configuration of your network. Network Agent installs on Windows, Solaris, and Linux. *Do not* install Network Agent on the FireWall-1 machine. When planning the deployment of Network Agent consider the following:
  - Network Agent must be able to directly *see* 2-way internet traffic from your internal network to filter and log effectively. Make sure your network configuration routes both the internet request *from* the workstation and the response from the internet back *to* the workstation past Network Agent.
  - The simplest deployment is to connect the Network Agent machine to an unmanaged, unswitched hub that is located between an external router and your network.



- If the Network Agent machine is connected to a switch or router, configure the switch or router to use bi-directional port spanning (mirroring).

If the span port on the switch or router is not capable of bi-directional communication, two network interface cards (NICs) are required in the installation machine: one NIC that can be configured for monitoring, attached to the span port; and a second NIC that can be configured for blocking, attached to a regular port. In this scenario, one NIC is receiving data, and one NIC is transmitting data, so the required two-way communication is provided by the two NICs in combination. After installation, the NICs must be configured for monitoring and blocking, respectively. For instructions, see the Network Agent chapter in the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

If you are installing Network Agent in a network that employs switches, see the Switched Configuration section in the Deploying Network Agent chapter of the *Deployment Guide* for Websense Enterprise/Web Security Suite for additional information.

- For small to medium sized organizations, Network Agent can be installed on the same server machine as the other Websense web filtering components, assuming that the server meets the minimum system requirements. For larger organizations, you may want to put Network Agent on a separate, dedicated server to increase the amount of traffic that can be managed.
- On larger networks, you may need to install multiple Network Agents and assign them to monitor various IP address ranges in your network. Make sure that the IP address ranges for each instance of Network Agent do not overlap. Overlapping IP ranges result in double logging. Deploy the Network Agents so that they can filter the entire network. Partial deployment results in incomplete filtering by protocol and bandwidth, as well as the loss of log data from network segments not watched by Network Agent. To define IP address ranges for multiple Network Agents, follow the instructions in the Network Agent chapter of the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

- Avoid deploying Network Agent across different LANs. If you install an instance of Network Agent on 192.x.x.x and configure it to communicate with a Filtering Service on 10.x.x.x through a variety of switches and routers, communication may be slowed enough to prevent Network Agent from blocking an internet request in time.
- Do *not* install Network Agent on a machine running any type of firewall. Network Agent uses a packet capturing utility which will not work properly when installed on a firewall machine. The only exception is a blade server or appliance with separate processors or virtual processors to accommodate Network Agent and the firewall software.
- ◆ **Usage Monitor:** Typically installed on the same machine as the Policy Server, but may be installed on a separate machine in your network that has access to the Policy Server machine. The Usage Monitor installs on Windows, Solaris, and Linux.



### Important

You can have only one installation of Usage Monitor for each Policy Server in your network.

---

- ◆ **Real-Time Analyzer (RTA):** Can be installed on the same machine as Filtering Service or on a separate machine. The Real-Time Analyzer installs on Windows only.

Real-Time Analyzer (RTA) can be memory and CPU demanding, depending on desired system settings and network load conditions. RTA should not be installed on real-time critical machines. For more information, see the *Deployment Guide* for Websense Enterprise/Web Security Suite.



### Important

You can have only one installation of RTA for each Policy Server in your network.

---

One of these web servers must be installed on the same machine as RTA

- Apache HTTP Server
- Microsoft IIS

**Note**

If you do not have one of the supported web servers on your system, the Websense installer provides the option of installing the Apache HTTP Server.

---

For information about supported versions of these web servers, see the *Deployment Guide* for Websense Enterprise/Web Security Suite.

- ◆ **Websense Transparent Identification Agents:** If you want to apply user- and group-based filtering policies, Websense software must be able to identify a user making a request, given the originating IP address. Installing a Websense transparent identification agent allows Websense software to filter internet requests from users in your directory service, without prompting users to log on to the browser. A transparent identification agent can be used if your integration product does not send user information for some or all users to the Websense Filtering Service.

DC Agent, eDirectory Agent, Logon Agent, and RADIUS Agent are the available Websense transparent identification agents. The following descriptions provide information about selecting and installing the appropriate agent(s) to identify users in your network.

- **DC Agent:** Installed in networks using a Windows directory service (NTLM-based or Active Directory). DC Agent can be installed on any Windows or Linux machine in the network, either on the same machine as other Websense components, or on a different machine.
  - For small to medium networks, Websense, Inc., recommends that you install only one DC Agent per domain. If you have a large, distributed network with many domain controllers on the same domain, you can install multiple DC Agents. Installing DC Agent on the domain controller machine is *not* recommended. DC Agent can be installed on any network segment as long as NetBIOS is allowed between the DC Agent and the domain controllers. Setting up the DC Agent in the DMZ is not recommended.
  - You may install DC Agent and RADIUS Agent together on the same machine or on separate machines in your network.
  - DC Agent and eDirectory Agent can be installed in the same network, but cannot be active at the same time, since Websense software does not support communication with both Windows and Novell directory services simultaneously. Do not install DC Agent and eDirectory Agent on the same machine.

- If DC Agent is not identifying all your users as anticipated, you may install Logon Agent as well to improve user authentication in your network. For example, this might be necessary in a network that uses Windows 98 workstations. DC Agent uses workstation *polling* to get user information from workstations as they make internet requests; however, polling cannot retrieve user information from a Windows 98 workstation.
- If you are installing DC Agent, be sure that the machine names of any Windows 9x workstations in your network do not contain any spaces. This situation could prevent DC Agent from receiving a user name when an internet request is made from that workstation.

For configuration information, see the User Identification chapter in the *Administrator's Guide* for Websense Enterprise/Web Security Suite. For detailed deployment information, see the white paper titled *Transparent Identification of Users in Websense Enterprise*, available at: [www.websense.com/docs/](http://www.websense.com/docs/).

- **eDirectory Agent:** Can be installed on the same machine as the rest of the Websense filtering software, or installed on a separate machine in your network. You can install multiple eDirectory Agents on the same network, each configured to communicate with the Filtering Service. You can install eDirectory and RADIUS Agent on the same machine or on separate machines in your network. The eDirectory Agent can be installed in the same network as DC Agent or Logon Agent, but cannot be active at the same time, since Websense software does not support communication with Windows and Novell directory services simultaneously. Do not install eDirectory Agent on the same machine as DC Agent or Logon Agent. The eDirectory Agent installs on Windows, Solaris, and Linux.

For configuration information, see the User Identification chapter in the *Administrator's Guide* for Websense Enterprise/Web Security Suite. For detailed deployment information, see the white paper titled *Transparent Identification of Users in Websense Enterprise*, available at: [www.websense.com/docs/](http://www.websense.com/docs/).

- **Logon Agent:** Can be installed on the same machine as the rest of the Websense filtering software, or installed on a separate machine in your network. Logon Agent may be installed together with DC Agent to improve the accuracy of user authentication in your network. Logon Agent installs on Windows, Linux, or Solaris and works together with the User Service and Filtering Service. Logon Agent can be used with a Windows NT-based directory service or with

Active Directory, which is LDAP-based. `LogonApp.exe`, the client application that passes user logon information to Logon Agent, runs only on Windows client machines. You must create a logon script to run `LogonApp.exe` in your network; see *Creating and Running the Script for Logon Agent*, page 196 for instructions. Logon Agent and eDirectory Agent can be installed in the same network, but cannot be active at the same time, since Websense software does not support communication with both Windows and Novell directory services simultaneously. Do not install Logon Agent and eDirectory Agent on the same machine.

For configuration information, see the User Identification chapter in the *Administrator's Guide* for Websense Enterprise/Web Security Suite. For detailed deployment information, see the white paper titled *Transparent Identification of Users in Websense Enterprise*, available at: [www.websense.com/docs/](http://www.websense.com/docs/).

- **RADIUS Agent:** Can be installed on the same machine as the rest of the Websense filtering software, or installed on a separate machine in your network. You may install multiple RADIUS Agents on the same network, each configured to communicate with the Filtering Service. RADIUS Agent can be used in conjunction with either Windows- or LDAP-based directory services. You can install RADIUS Agent and eDirectory Agent on the same machine or on separate machines in your network. The RADIUS Agent installs on Windows, Solaris, and Linux.

For configuration information, see the User Identification chapter in the *Administrator's Guide* for Websense Enterprise/Web Security Suite. For detailed deployment information, see the white paper titled *Transparent Identification of Users in Websense Enterprise*, available at: [www.websense.com/docs/](http://www.websense.com/docs/).

- ◆ **Remote Filtering components**

The Remote Filtering components are required only if you need to enable web filtering on user workstations located outside your organization's network firewall or internet gateway. They can be installed from a **Custom** installation only.

**Note**

To enable the Remote Filtering components, you must subscribe to the remote filtering service.

---

- **Remote Filtering Server:** Should be installed on a separate, dedicated machine. This machine must be able to communicate with the Filtering Service and with Remote Filtering Clients on user workstations that may be used both inside and outside the network firewall. The Remote Filtering Server installs on Windows, Linux, and Solaris.

The Remote Filtering Server automatically detects whether clients are inside or outside of the network firewall. If it determines that a client is inside the firewall, the user is filtered just like other internal clients. Remote Filtering is only activated if the client is outside the firewall.

To provide failover protection for the primary Remote Filtering Server, you can install secondary and tertiary Remote Filtering Servers. If a Remote Filtering Client on a remote workstation cannot connect with the primary Remote Filtering Server, it will try to connect with the secondary, then the tertiary, then the primary again, and so on.

- Install only one primary Remote Filtering Server for each Filtering Service in your network.
- Do not install the Remote Filtering Server on the same machine as the Filtering Service or Network Agent.
- The Remote Filtering Server machine does not have to be joined to a domain.

Remote Filtering components are not included in the deployment diagrams provided in this chapter. For deployment information and network diagrams, see the Remote Filtering section in the *Deployment Guide* for Websense Enterprise/Web Security Suite.

- **Remote Filtering Client:** Can be installed on user machines that you want to filter outside the network firewall. To deploy this client application, you can use the provided installer, called the **Remote Filtering Client Pack**, and a third-party deployment tool. A Remote Filtering Client must be able to communicate with a Remote Filtering Server inside the network firewall to enable web filtering on the

remote workstation. The Remote Filtering Client Pack and the Remote Filtering Client install only on Windows.

**Note**

The Remote Filtering Client is also available as part of the Websense Client Policy Manager™ (CPM). If you are using CPM to manage application filtering on employee desktops, the Remote Filtering Client is provided as part of the CPM Client Agent. For more information, see your Websense Client Policy Manager documentation.

---

Remote Filtering components are not included in the deployment diagrams provided in this chapter. For detailed deployment information and network diagrams, see the Remote Filtering section in the *Deployment Guide* for Websense Enterprise/Web Security Suite.

**Important**

Do not install the Remote Filtering Client on a Remote Filtering Server machine.

---

- ◆ **Websense Reporting components:** Should be installed on a separate machine from the Websense Enterprise/Web Security Suite web filtering components, except when evaluating Websense software, or in a small network (see the *Deployment Guide* for detailed system requirements and recommendations). The Log Server receives and saves information about internet requests filtered by Websense Enterprise/Web Security Suite. Reporter and Explorer then use this information to create reports on users' internet activity. See the Websense Enterprise/Web Security Suite Reporting documentation for installation and administrative information.

**Note**

To properly generate reports, you must use the same version of the Websense Reporting Tools as the Websense Enterprise/Web Security Suite software.

---

## Deploying Websense Components with your Integration Product

---

Before beginning installation, read the *Deployment Guide* for Websense Enterprise/Web Security Suite to learn about system requirements and how best to deploy Websense Enterprise/Web Security Suite components, as well as the Websense Reporting Tools, in your network.

Websense components can be installed on a dedicated server machine, or widely distributed across a network on various operating systems. The recommended deployment depends on a number of factors, including the size and complexity of your network, the amount of traffic being handled, and the types of hardware available. Wherever you decide to deploy Websense components, make sure that the installation machine can handle the expected traffic load.

The information in this section is not intended to be a comprehensive discussion of all available deployment options. The network architecture shown represents a small network, with 500 users or fewer. The network diagrams are intended primarily to show the recommended location of your **integration product** relative to the Websense components. The network architecture represents a small network, with 500 users or fewer. The network diagram is intended primarily to show the recommended location of your **integration product** relative to the Websense components. For detailed information about where to deploy individual Websense components in networks of all sizes, see the *Deployment Guide* for Websense Enterprise/Web Security Suite.

The following is a general discussion of two common deployment options: the simple deployment with unified components, and the complex deployment with distributed components.

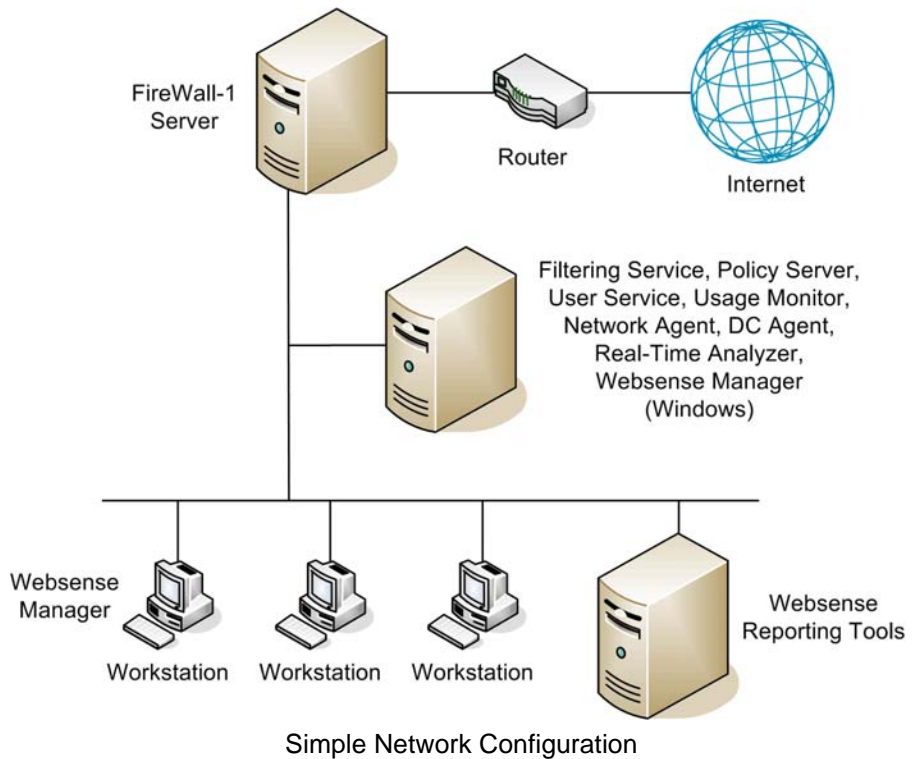
### Simple

In the simplest and most common network topology, an organization has one firewall that resides on a dedicated server. All the Websense Enterprise or Web Security Suite components are installed on a separate machine on the internal network. If Network Agent is installed on the same machine as the other components, that machine must be able to directly see internet traffic on your internal network.

Websense Manager can be installed on the same machine as the other components, and on any Windows, Linux, or Solaris workstation with network



access to the Websense machine. You may want to install additional instances of Websense Manager in your network for convenience, as shown in the diagram.

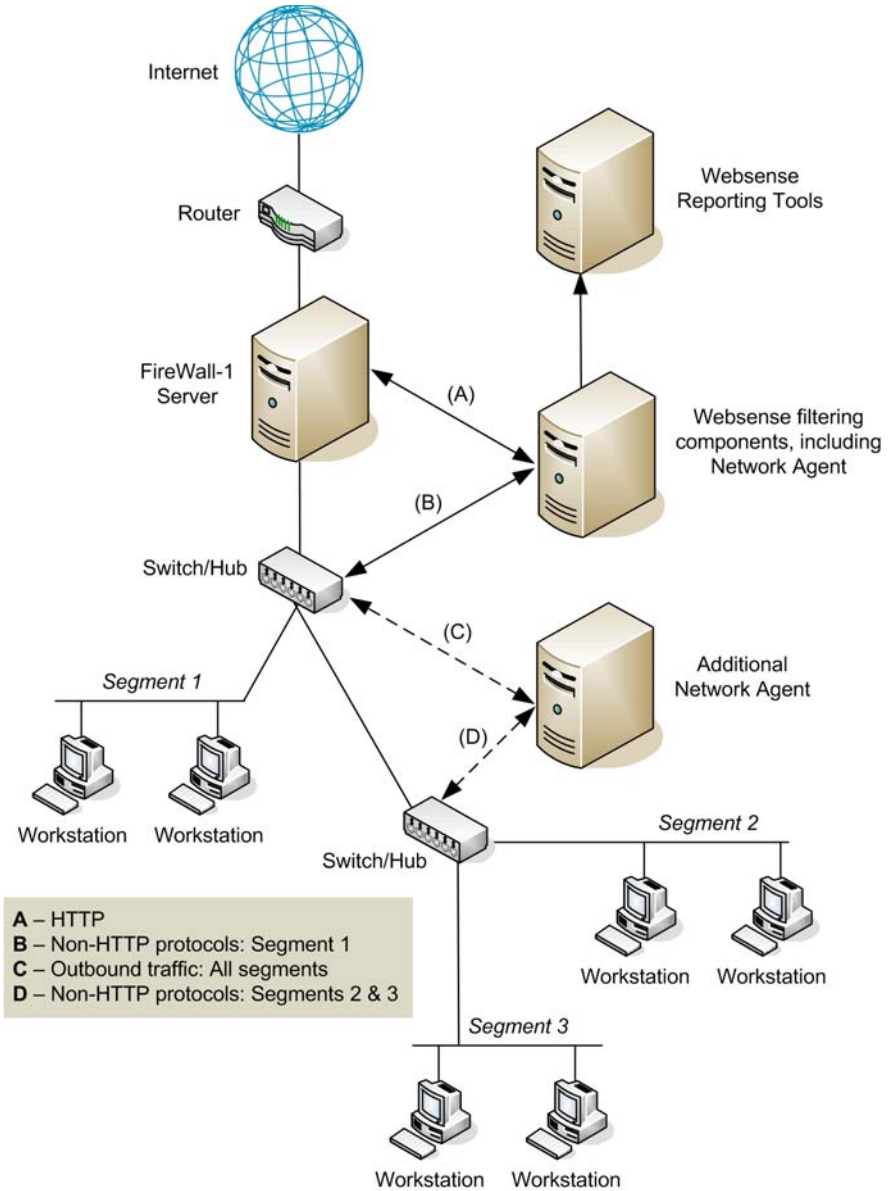


## Distributed

Larger systems (more than 1000 users) may require distributed deployment for such things as load balancing and multilingual support. You may find it necessary to install multiple Network Agents to detect outbound traffic on individual network segments, or multiple Websense Managers to allow administration from convenient locations across the network.

In environments with a large number of workstations, installing multiple Filtering Services for load balancing purposes may be appropriate; however, some load balancing configurations permit the same user to be filtered by different Filtering Service installations, depending on the current load. For information about how to configure Websense software in this situation, see the deployment instructions for multiple Filtering Service environments in the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

In the following diagram, Websense software is installed on a single machine in a central location where it can manage both protocol and HTTP traffic. HTTP requests are handled by FireWall-1, and the non-HTTP traffic is managed by Network Agent, which is positioned to detect all outbound traffic.



Multi-Segmented Network Configuration

Do not install Websense components on the same machine as FireWall-1, as this can cause performance and security issues. Network Agent will not function correctly if installed on the FireWall-1 machine.

**Warning**

Websense, Inc., and Check Point do not recommend installing Websense Enterprise or Web Security Suite and FireWall-1 on the same machine. *Do not* install Network Agent on the same machine as FireWall-1.

---

The exception is installing on a blade server that has separate processors to accommodate Websense components and the Firewall-1 software.

## Websense Reporting Components

Websense, Inc., does not recommend installing Websense Reporting components on the same machine as Websense Enterprise/Web Security Suite. Filtering and logging functions are CPU intensive and could cause operating system errors. Install Websense Enterprise/Web Security Suite and Websense Reporting components on separate machines inside the network, where they will not have to compete for resources. The exception to this is when Websense Enterprise/Web Security Suite is being evaluated on a small network or segment of a larger network.

For detailed information about how to deploy each of the Websense Reporting components in your network, see the *Deployment Guide* for Websense Enterprise/Web Security Suite, and your Websense Enterprise/Web Security Suite Reporting documentation.

## Directory Services

If your environment includes a directory service, Websense software allows you to filter internet requests based on individual policies assigned to directory objects. Directory objects identified in a directory service can be added in Websense Manager and assigned specific policies.

Websense software can communicate with the following directory services:

- ◆ Windows® NTLM-based directories
- ◆ Windows® Active Directory®

- ◆ Sun Java™ System Directory Server
- ◆ Novell Directory Services®/Novell® eDirectory®

For information about supported versions of these directory services, see the *Deployment Guide* for Websense Enterprise/Web Security Suite. For information about configuring directory service access, see the *Administrator's Guide* for Websense Enterprise/Web Security Suite.



**Note**

Websense software can communicate with your directory service whether it runs on the same operating system as the Websense components, or on a different system.

---

Filtering can be based on individual user, group, and domain/organizational unit policies, providing that the Websense software is able to identify the user making an internet request. The authentication method you configure must allow Filtering Service to obtain directory object information from a Windows or LDAP directory. For information about accessing LDAP and Windows directories, see the *Administrator's Guide* for Websense Enterprise/Web Security Suite.



**Note**

In any environment, Websense software can filter based on workstation or network policies. Workstations are identified within the Websense software by their IP addresses, and networks are identified as IP address ranges.

---

Internet requests can be filtered based on policies assigned to individual directory objects after the following tasks have been accomplished:

- ◆ If you are using the Sun Java System Directory Server or Novell Directory Services/eDirectory:
  1. Enable the appropriate directory service in Websense Manager.
  2. Enable the Websense software to identify users transparently with Novell by installing and configuring the Websense eDirectory Agent.

3. Enable Websense manual authentication so that if the Websense software is unable to identify users transparently, it will prompt users to manually authenticate.

Detailed instructions for each of these tasks can be found in the User Identification chapter in the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

- ◆ If you are using a Windows NTLM-based directory or Active Directory:
  1. Configure the Windows directory service in Websense Manager.
  2. Enable the Websense software to identify users transparently by installing and configuring the Websense DC Agent and/or Logon Agent.
  3. Enable Websense manual authentication so that if the Websense software is unable to identify users transparently, it will prompt users to manually authenticate.

Detailed instructions for each of these tasks can be found in the User Identification chapter in the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

**Note**

DC Agent on Linux is not supported with LDAP-based directory services. If you are running DC Agent on Linux and are using Windows Active Directory, NTLM authentication must be enabled in Active Directory.

---

The Websense transparent identification feature allows the Websense software to filter internet requests from users in a Windows or Novell directory service, without prompting users to manually authenticate. Websense software can transparently identify users in a Windows domain if DC Agent and/or Logon Agent is installed. In networks using a Novell directory service, you can transparently identify users by installing the Websense eDirectory Agent. If users access your network through a RADIUS server, you use RADIUS Agent to transparently identify them. RADIUS Agent can be used in conjunction with either Windows- or LDAP-based directory services.

Once the Websense Filtering Service is configured to communicate with the transparent identification agent (DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent), the agent obtains user information from the directory service and sends the information to Filtering Service. When Filtering Service

receives the IP address of a machine making an internet request, Filtering Service matches the address with the corresponding user name provided by the transparent identification agent. This allows the Websense software to transparently identify users whenever they open a browser that sends an internet request to your integration product.

For more information about transparent identification using DC Agent, Logon Agent, eDirectory Agent, and RADIUS Agent, see the User Identification chapter in the *Administrator's Guide* for Websense Enterprise/Web Security Suite. For more detailed information, see the white paper titled *Transparent Identification of Users in Websense Enterprise*, available at: [www.websense.com/docs/](http://www.websense.com/docs/).

## Filtering in a Network with Citrix® Server Users

If your network includes some users who access the internet via a Citrix® server, and others who access the internet through another gateway (firewall, caching appliance, or proxy server), you must install two complete instances of Websense software:

- ◆ One instance of Websense software choosing the Citrix integration, to filter Citrix users. Follow the instructions in the *Installation Guide for use with Integrated Citrix® Servers*.
- ◆ Another, separate instance of Websense software, to filter the non-Citrix users. This instance of Websense software can be integrated with the other gateway (firewall, caching appliance, or proxy server), or it can be the Websense Stand-Alone Edition. To install this Websense instance, follow the instructions in the Websense Enterprise/Web Security Suite Installation Guide for the integration product you are using, or for the Stand-Alone Edition.

## System Requirements

---

Websense software can be installed on machines with Windows, Solaris, and Linux operating systems (see the *Deployment Guide* for supported versions). Not all Websense components are supported on all three types of operating system. However, you can install Websense components on machines with different operating systems, and they will be able to communicate with one another. For example, an instance of Websense Manager installed on a Windows machine can configure a Policy Server installed on a Windows,

Solaris, or Linux machine. For a list of supported operating systems for each Websense Enterprise/Web Security Suite component, see the *Deployment Guide* for Websense Enterprise/Web Security Suite.

Such factors as network size, network configuration, and internet traffic volume can affect the ability of Websense software to filter internet requests. For hardware recommendations for your network, see the *Deployment Guide* for Websense Enterprise/Web Security Suite.

For a complete list of system requirements for installation of Websense Enterprise/Web Security Suite components in your network, see the *Deployment Guide* for Websense Enterprise/Web Security Suite. This section contains system requirements specific to your integration product.

## Supported Check Point FireWall-1 Versions

- ◆ Citrix Presentation Server

Websense Enterprise and Web Security Suite v6.3.1 are compatible with the following versions of FireWall-1:

- ◆ FireWall-1 NG, Feature Pack 1 to Feature Pack 3
- ◆ FireWall-1 NG with Application Intelligence (AI)
- ◆ FireWall-1 NGX

Contact Check Point if you need assistance determining which FireWall-1 version is running.

## User Workstations

Websense filtering is based on protocols, not on the operating system of the user workstation being filtered.

To be filtered by the Websense software, a user workstation must access the internet through Check Point FireWall-1.

Browsers must be set to use FireWall-1 as the default gateway.





# Upgrading Websense Enterprise/Web Security Suite

This chapter contains procedures for upgrading a previous version of Websense Enterprise/Web Security Suite to version 6.3.3. It also contains instructions for upgrading an existing Websense Stand-Alone Edition to a Websense system integrated with Check Point FireWall-1.

Before upgrading, make sure your system meets the system requirements listed in the *Deployment Guide* for Websense Enterprise/Websense Web Security Suite.

The Websense Enterprise/Web Security Suite installer will upgrade all Websense Enterprise/Web Security Suite components detected on the installation machine, with the exception of the Remote Filtering Client.

**Note**

If the optional Remote Filtering Client application is installed on user workstations in your network, see [Remote Filtering Client](#), page 50 for upgrade instructions.

---

Direct upgrades from version 6.1 or higher are supported. Websense Enterprise/Web Security Suite “version 6.1 or higher” refers to the following releases:

- ◆ 6.1.x
- ◆ 6.2.x
- ◆ 6.3.x

During upgrade, the installer will configure v6.3.3 components to use the same network interface cards (NICs) for Websense communications and the same Network Agent used by the earlier version. The installer will also automatically assign the same port numbers to the v6.3.3 Websense components that the existing Websense components use.

The Websense Master Database will be removed during upgrade. You can either download the new Master Database during upgrade of the Filtering Service, or download it after the upgrade is complete by using Websense Manager. When scheduling the upgrade, be aware that users will not be filtered until the services are restarted and the new Master Database has been successfully loaded. Depending on how your integration product is configured to respond when Websense filtering is unavailable, traffic will either be allowed unfiltered or blocked entirely during the upgrade.



### Note

The upgrade process is for use on properly functioning Websense systems. Upgrading will not repair a non-functional system.

---

## Versions Supported

---

Direct upgrades from v6.1 or higher of Websense Enterprise/Web Security Suite are supported. If you are running v5.2 or v5.5, an upgrade to v6.3.3 requires two steps: upgrade to v6.1 first, and then upgrade to v6.3.3.

To perform the intermediate upgrade to v6.1, you will need the v6.1 installer for your product and operating system. Download the appropriate installer:

- ◆ **Websense Enterprise v6.1 installer:**
  - **Windows:** [www.websense.com/Downloads/files/v6.1/full/Websense61Setup.exe](http://www.websense.com/Downloads/files/v6.1/full/Websense61Setup.exe)
  - **Solaris:** [www.websense.com/Downloads/files/v6.1/full/Websense61Setup\\_Slr.tar.gz](http://www.websense.com/Downloads/files/v6.1/full/Websense61Setup_Slr.tar.gz)
  - **Linux:** [www.websense.com/Downloads/files/v6.1/full/Websense61Setup\\_Lnx.tar.gz](http://www.websense.com/Downloads/files/v6.1/full/Websense61Setup_Lnx.tar.gz)
- ◆ **Websense Web Security Suite v6.1 installer:**
  - **Windows:** [www.websense.com/Downloads/files/v6.1/full/WebSecurity61\\_Setup.exe](http://www.websense.com/Downloads/files/v6.1/full/WebSecurity61_Setup.exe)
  - **Solaris:** [www.websense.com/Downloads/files/v6.1/full/WebSecurity61\\_Setup\\_Slr.tar.gz](http://www.websense.com/Downloads/files/v6.1/full/WebSecurity61_Setup_Slr.tar.gz)
  - **Linux:** [www.websense.com/Downloads/files/v6.1/full/WebSecurity61\\_Setup\\_Lnx.tar.gz](http://www.websense.com/Downloads/files/v6.1/full/WebSecurity61_Setup_Lnx.tar.gz)

If you are running Websense Enterprise v5.0, v5.0.1, or v5.1, Websense, Inc., recommends that you perform a fresh installation of v6.3.3 rather than upgrading. If you decide to upgrade to v6.3.3, three steps are required: upgrade to v5.5.2 first, then upgrade to v6.1, and finally upgrade to v6.3.3.

The v5.5.2 Websense Enterprise installer for your operating system can be downloaded from:

- ◆ **Windows:** [www.websense.com/Downloads/files/v5.5.2/full/Websense552Setup.exe](http://www.websense.com/Downloads/files/v5.5.2/full/Websense552Setup.exe)
- ◆ **Solaris:** [www.websense.com/Downloads/files/v5.5.2/full/Websense552Setup\\_Slr.tar.gz](http://www.websense.com/Downloads/files/v5.5.2/full/Websense552Setup_Slr.tar.gz)
- ◆ **Linux:** [www.websense.com/Downloads/files/v5.5.2/full/Websense552Setup\\_Lnx.tar.gz](http://www.websense.com/Downloads/files/v5.5.2/full/Websense552Setup_Lnx.tar.gz)

If you are running Websense Enterprise v4.4.1 or earlier, contact Websense Technical Support for upgrade assistance.

---

## Transferring Configuration Data Without Upgrading

---

The recommended path for upgrading Websense Enterprise/Web Security Suite is through the normal upgrade process, in which all configuration data from the earlier version is retained. In some cases, however, you may decide that an upgrade of your production system is undesirable. Your network policy may not permit upgrades to the production system, or you may want to move your Websense software to a larger machine to accommodate increased network traffic.

If running a normal upgrade is not an option, you can use either of two procedures that will transfer configuration data from the production system to a freshly installed version of Websense Enterprise/Web Security Suite. These procedures require a test environment and may involve several cycles of installation and upgrade.



### Warning

Do not attempt to upgrade an earlier version of Websense Enterprise/Web Security Suite by copying the `config.xml` file into a v6.3.3 system. Configuration files from earlier versions are not compatible with v6.3.3.

---

The procedures for converting to v6.3.3 without upgrading are described in the technical paper titled *Transferring Configuration Settings to a v6.3.3 System Without Upgrading*, available at: [www.websense.com/docs/](http://www.websense.com/docs/).

## Before You Upgrade

---

- ◆ **Backing up files:** Before upgrading to a new version of Websense Enterprise/Web Security Suite, Websense, Inc., recommends that you perform a full system backup as a fallback strategy. This will allow you to restore your current production system with a minimum of downtime should you encounter any problems with the upgrade. At a minimum, you should back up the latest Websense configuration file and the initialization files. To back up these files, stop the Policy Server and copy the `config.xml` file, the `websense.ini` file, and the `eimserver.ini` file from the `Websense\bin` folder to a safe location.
- ◆ **Non-English language versions:** In v6.3.3, all Websense installers are available in English and nine other language versions (see [Non-English Language Versions](#), page 73). When upgrading, choose the v6.3.3 installer for the language of your current Websense installation. Upgrading your system with the v6.3.3 installer for a non-English language will first convert the system to English. At the end of the upgrade process, the v6.3.3 Language Pack installer will run automatically to convert the upgraded Websense components to your language.



### Note

All Websense components in a Websense installation must be in the same language.

---

- ◆ **Upgrading distributed components:** To upgrade your system, you must run the Websense installer on each machine on which a Websense component resides.



### Warning

Always run the installer on the **Policy Server** machine first. The Policy Server must be successfully upgraded and running before you upgrade or install other Websense components in your network.

---

- ◆ **Remote Control Utilities:** Upgrade of Websense software using a remote control utility such as Terminal Services is not supported.
- ◆ **Reporting:** To properly generate reports, you must use the same version of Websense filtering software and Websense Reporting Tools.



### Important

Upgrade all Websense Enterprise/Web Security Suite components *before* upgrading your existing Websense Enterprise Reporting or Web Security Suite Reporting components.

---

For information about upgrading Reporting components, see the *Reporting Installation Guide* for Websense Enterprise/Web Security Suite.

- ◆ **Upgrading FireWall-1:** If you decide to upgrade your version of FireWall-1, do so *before* upgrading your Websense system. When you upgrade from an earlier supported version of FireWall-1 to a later supported version—for example, from FireWall-1 NG to FireWall-1 NGX—your configuration settings from the earlier version are preserved, and the firewall is configured to communicate with Websense software with a *clear connection* (the default). No further configuration of FireWall-1 is required to begin filtering with the new version of Websense software.
- ◆ **Websense services:** Websense services must be running when the upgrade process begins. The installer will stop and start these services as necessary during the upgrade. If these services have been running uninterrupted for several months, however, the installer may not be able to stop them before the upgrade process times out. To ensure the success of the upgrade, manually stop and restart all the Websense services before beginning the upgrade.



### Note

If you have set the **Recovery** properties of any of your Websense services to restart the service on failure, you must change this setting to **Take No Action** before upgrading.

---

- ◆ **Matching locales:** When upgrading a Filtering Service that is installed on a different machine from Websense Manager, you must upgrade the Filtering Service to v6.3.3 in the same locale environment (language and character set) as the Websense Manager.
  - When upgrading Filtering Service on Windows, open **Control Panel > Regional Options** and change the locale to match that of the Websense Manager machine before beginning the upgrade.
  - When upgrading on Solaris or Linux, log on to the Filtering Service machine with the locale appropriate to the Websense Manager.

Once the upgrade is complete, the Websense services can be restarted with any locale setting.

## Upgrading on Windows

---

Before upgrading to a new version of Websense Enterprise/Web Security Suite, Websense, Inc., recommends that you perform a full system backup as a fallback strategy. This will allow you to restore your current production system with a minimum of downtime should you encounter any problems with the upgrade.

At a minimum, be sure you have backed up the following files before proceeding:

- ◆ `websense.ini`
- ◆ `eimserver.ini`
- ◆ `config.xml`



### Important

If your Websense services have been running uninterrupted for several months, the installer may have difficulty stopping them. To prevent the upgrade process from timing out and failing, stop the services manually and restart them again before beginning the upgrade. For instructions, see [Stopping or Starting Websense Services](#), page 185.

---

To upgrade your Websense Enterprise/Web Security Suite v6.1 or higher system to v6.3.3:

1. Close all Websense Managers anywhere in the network that connect to the Policy Server you are upgrading.
2. Log on to the installation machine with **domain** and **local** administrator privileges.

If you are upgrading User Service and DC Agent, this will assure that they have administrator privileges on the domain.



### Important

User Service and DC Agent must have administrator privileges on the network to retrieve user login information from the domain controller. Without this information, Websense software cannot filter by users and groups. If you cannot install these components with such privileges, you can configure domain administrator privileges for these services after installation. For instructions, see *Configure Domain Administrator Privileges*, page 207.

---

3. Close all applications and stop any antivirus software.



### Warning

Be sure to close the Windows Event Viewer, or the upgrade may fail.

---

4. Obtain an installer package for Websense Enterprise/Web Security Suite:  
**Web download:** To download an installer package, go to [www.websense.com](http://www.websense.com), and then navigate to the Downloads page.

- a. Choose the dynamic (online) or full (offline) installer package, the operating system, and the language.



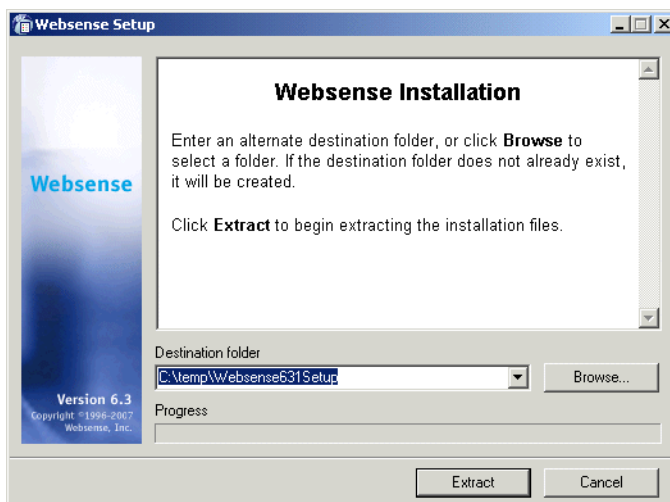
**Note**

The **Dynamic** installer is an **online** installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.

The **Full** installer is a complete **offline** installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install the Websense Enterprise/Web Security Suite components. Use this package if you experience difficulties with the online installer.

- b. Download the selected installer package to a folder on the installation machine, and double-click to extract the installer files.

A screen displays instructions for extracting the setup program.



Websense Installer File Extraction

5. If you do not want to accept the default location, click **Browse** to select a destination folder, or type in a path.



If the path you enter does not exist, the installer will create it for you.



---

### Important

Do not extract the installer files to a folder on your desktop. This may prevent the Real-Time Analyzer from receiving the IP address of the Policy Server machine. Accept the default location of `C:\temp` or select another appropriate folder.

---

6. Click **Extract** to begin decompressing the files.
  - If Websense installation files already exist in that location, you may choose to overwrite the existing files.
  - A progress bar shows the status of the extraction, and the view pane scrolls a list of the files as they are decompressed.
  - `Setup.exe` runs automatically after the files are decompressed.

7. Follow the onscreen instructions and click **Next** to advance through the welcome screen and the subscription agreement.

The installer detects the Websense components from your earlier version and asks how you want to proceed. You can upgrade the current system or exit the installer.

8. Select **Upgrade** and click **Next**.

A list of currently running Websense services from the earlier version appears. A message explains that the installer must stop these services before the upgrade can proceed.

9. Click **Next** to continue.

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer quits.
- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary screen appears, listing the installation path, file sizes, and the components that will be upgraded.

10. Click **Next** to begin the upgrade.
  - The Download Manager copies the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.
  - If you are using the Apache HTTP Server, you must restart it before using the Real-Time Analyzer on your upgraded system. The installer asks if you want to restart Apache now or wait until later. Select **Yes** or **No** and click **Next** to continue.

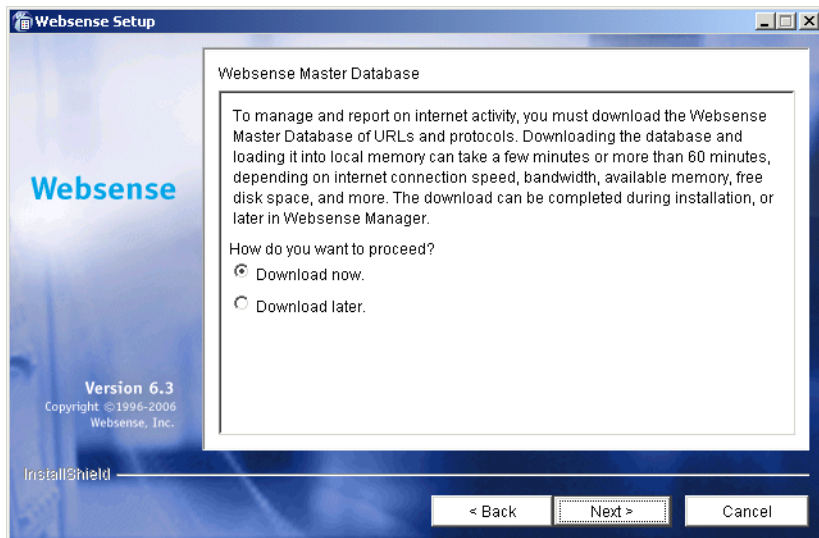
The installer asks if you want to download the Websense Master Database now or at a later time using Websense Manager.



### **Warning**

During upgrade, the installer removes the existing Master Database. Websense filtering cannot resume until the new Master Database has been successfully downloaded, decompressed, and loaded. This may take a few minutes or more than 60 minutes, depending on factors such as internet connection speed, bandwidth, available memory, and free disk space.

---

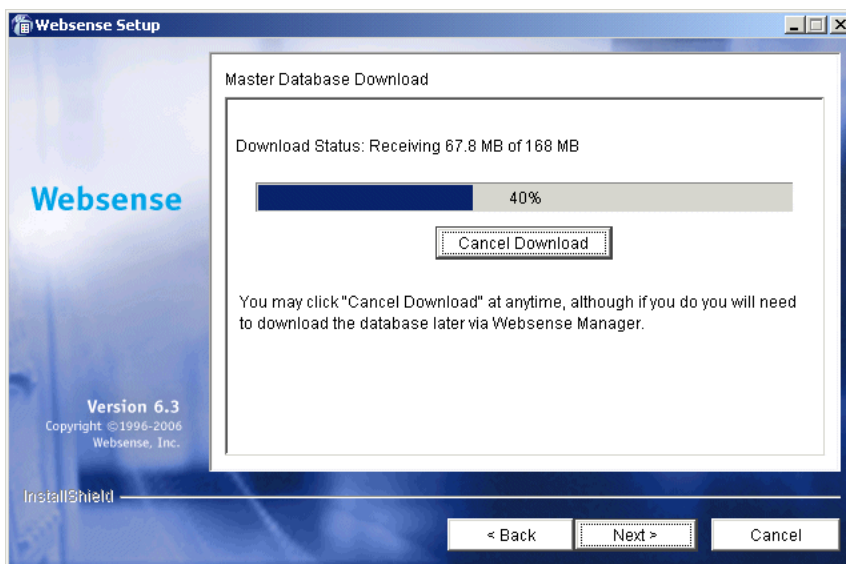


Master Database Download Selection Screen

11. Select a database download option and click **Next**.

If you have chosen to download the Master Database now, a progress bar appears. The database must first be downloaded from the internet, and then decompressed and loaded into local memory. Downloading the database from the internet can take a few minutes or more than 30 minutes, depending on factors such as internet connectivity, bandwidth, time of day, and your location relative to the download server.

Decompressing and loading the database can take a few minutes or more than 30 minutes, depending on factors such as available memory, free disk space, and server process utilization.



Master Database Download Progress

When the database has finished loading, a message appears advising you of the status of the download. Click **Next** to continue.

12. When a message announcing successful completion of the installation is displayed:
  - If you chose a non-English language installer, click **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions to update Websense components with text in the selected language.
  - If you chose an English language installer:
    - If Websense Manager was not upgraded, no further action is required and you can click **Finish** to exit the installer.
    - If Websense Manager was upgraded, click **Next** to continue. The installer displays a screen asking if you want to launch Websense Manager. If you do not want to launch Manager, clear the checkbox. Click **Finish** to exit the installer.
13. If you stopped your antivirus software, be sure to start it again.

14. Update the FireWall-1 dictionary with new Websense settings, and update the Websense Resource Object in FireWall-1 before you begin filtering with the new version of Websense software. For more information, see *Chapter 7: Configuring FireWall-1 NG, NG with AI, and NGX*.



### Important

Make sure you upgrade any other Websense components or products that may have a dependency on the system you just upgraded. This will prevent conflicts caused by incompatible versions.

For example, if you are using the Websense Reporting Tools, you must upgrade them to the same version as your Websense filtering software to properly generate reports.

---

If you decide to change the location of a Websense component, add a feature, or remove a component, run the Websense installer again on the machine you want to modify and select the appropriate option. The installer detects the presence of Websense components and offers you options for modifying your installation.

## Upgrading on Solaris or Linux

---

Before upgrading to a new version of Websense Enterprise/Web Security Suite, Websense, Inc., recommends that you perform a full system backup as a fallback strategy. This will allow you to restore your current production system with a minimum of downtime should you encounter any problems with the upgrade.

At a minimum, be sure you have backed up the following files before proceeding:

- ◆ `config.xml`
- ◆ `eimserver.ini`
- ◆ `websense.ini`



### Important

If your Websense services have been running uninterrupted for several months, the installer may have difficulty stopping them. To prevent the upgrade process from timing out and failing, stop the services manually and restart them again before beginning the upgrade.

---

To upgrade Websense Enterprise/Web Security Suite v6.1 or higher to v6.3.3:

1. Close all Websense Managers anywhere in the network that connect to the Policy Server you are upgrading.
2. Log on to the installation machine as the **root** user.
3. Close all applications and stop any antivirus software.
4. Create a setup directory for the installer files.

For example: `/root/Websense_setup`

5. Obtain an installer package for Websense Enterprise/Web Security Suite:

**Web download:** To download an installer package, go to [www.websense.com](http://www.websense.com), and then navigate to the Downloads page.

- a. Choose the dynamic (online) or full (offline) installer package, the operating system, and the language.
- 



### Note

The **Dynamic** installer is an **online** installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.

The **Full** installer is a complete **offline** installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install the Websense Enterprise/Web Security Suite components. Use this package if you experience difficulties with the online installer.

---

- b. Save the selected installer package to the setup directory on the installation machine.

6. In the setup directory, enter the following command to unzip the file:

```
gunzip <download file name>
```

For example: `gunzip Websense63Setup_Slr.tar.gz`

7. Expand the file into its components with the following command:

```
tar xvf <unzipped file name>
```

For example: `tar xvf Websense63Setup_Slr.tar`

This places the following files into the setup directory:

File	Description
install.sh	Installation program.
Setup	Archive file containing related installation files and documents.
Documentation	Release Notes: An HTML file containing release notes and last minute information about the Websense software. Read this file with any supported browser.

8. Run the installation program from the setup directory with the following command:

```
./install.sh
```

To run the GUI version of the installer, use the following command:

```
./install.sh -g
```

If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.

9. Follow the onscreen instructions through the subscription agreement.

10. Follow the upgrade sequence:

- **Websense upgrade:** The installer detects the earlier version of Websense components and gives you the choice of upgrading the existing installation or exiting Setup. Be sure to close any Websense Managers connected to the Policy Server being upgraded before continuing. Select **Upgrade** and continue.
- **Stopping Websense services:** A list of currently running Websense services from the earlier version appears. A message explains that the installer must stop these services before the upgrade can proceed. Select **Next** to continue.

- **System requirements check:** The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.
    - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
    - If the installation machine has less than the recommended amount of memory, the installation will continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.
  - **Installation summary:** A summary list appears, showing the installation path, installation size, and the components to be upgraded.
11. Select **Next** to begin the upgrade.
- The Download Manager copies the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.
  - **Master Database Download:** The installer asks if you want to download the Websense Master Database now or at a later time using Websense Manager. Select a database download option and then select **Next** to continue.



### Warning

During upgrade, the installer removes the existing Master Database. Websense filtering cannot resume until the new Master Database has been successfully downloaded, decompressed, and loaded. This may take a few minutes or more than 60 minutes, depending on factors such as internet connection speed, bandwidth, available memory, and free disk space.

---

If you have chosen to download the Master Database now, the download begins. The database must first be downloaded from the internet, and then decompressed and loaded into local memory. Downloading the database from the internet can take a few minutes or more than 30 minutes, depending on factors such as internet connectivity, bandwidth, time of day, and your location relative to the



download server. Decompressing and loading the database can take a few minutes or more than 30 minutes, depending on factors such as available memory, free disk space, and server process utilization.

When the database has finished loading, a message appears advising you of the status of the download. Select **Next** to continue.

12. When a message announcing successful completion of the installation is displayed:
  - If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions to update Websense components with text in the selected language.
  - If you chose an English language installer:
    - If you are installing in GUI mode, and Websense Manager was upgraded, select **Next** to continue. The installer asks if you want to start Websense Manager. Make a choice and select **Finish** to exit the installer.
    - Otherwise, select **Finish** to exit the installer.
13. If you stopped your antivirus software, be sure to start it again.
14. Update the FireWall-1 dictionary with new Websense settings, and update the Websense Resource Object in FireWall-1 before you begin filtering with the new version of Websense software. For more information, see [Chapter 7: Configuring FireWall-1 NG, NG with AI, and NGX](#).



### Important

Make sure you upgrade any other Websense components or products that may have a dependency on the system you just upgraded. This will prevent conflicts caused by incompatible versions.

For example, if you are using Websense Reporting Tools, you must upgrade them to the same version as the Websense filtering components to properly generate reports.

---

If you decide to change the location of a Websense component, add a feature, or remove a component, run the Websense installer again on the machine you want to modify and select the appropriate option. The installer detects the

presence of Websense components and offers you options for modifying your installation.

## Upgrading the Remote Filtering Components

---

If the optional Remote Filtering components are installed in your network, you must upgrade them along with the rest of your Websense Enterprise/Web Security Suite components.



### Important

You must upgrade Remote Filtering Server to the same version as the rest of your Websense components.

Remote Filtering Server 6.3.3 is backwards compatible with Remote Filtering Client 6.2. You do not have to upgrade your v6.2 Remote Filtering Clients to v6.3.3, but be aware that they will not be able to access the remote filtering features added in version 6.3.3. For information about these features, see the *Websense Enterprise and Websense Web Security Suite v6.3.3 Release Notes*.

---

## Remote Filtering Server

The Remote Filtering Server is upgraded in the same manner as the rest of the Websense components, by running the v6.3.3 Websense installer on the machine where the Remote Filtering Server is installed. See the previous sections of this chapter for detailed instructions.

## Remote Filtering Client Pack

The Remote Filtering Client Pack can be upgraded in the same manner as the rest of the Websense components, by running the v6.3.3 Websense installer on the machine where the Remote Filtering Client Pack is installed. See the previous sections of this chapter for detailed instructions.

## Remote Filtering Client

The Remote Filtering Clients in your network can be upgraded in two ways:

- ◆ **Manual upgrade:** Use the v6.3.3 Remote Filtering Client Pack installer package to manually uninstall the existing version of the Remote Filtering Client on an individual workstation, and then install the new version. See [Manual Upgrade of Remote Filtering Client, page 51](#) for information. This upgrade method does *not* preserve existing Remote Filtering Client configuration settings; communication information for Remote Filtering Server must be re-entered.
- ◆ **Automatic upgrade with third-party tool:** Use the v6.3.3 Remote Filtering Client Pack and a third-party deployment tool to automatically uninstall the existing version of Remote Filtering Client on employee workstations, and replace it with the new version. See [Upgrading Remote Filtering Client with a Third-Party Deployment Tool, page 53](#) for information.



**Note**

If you add Websense Client Policy Manager (CPM) to your network when you upgrade, you do not have to upgrade your Remote Filtering Clients as described in this section. Because the Remote Filtering Client is included as part of the CPM Client Agent, you can simply deploy CPM Client Agent with the appropriate remote filtering settings. For more information, see your Websense Client Policy Manager documentation.

---

## Manual Upgrade of Remote Filtering Client

To manually upgrade an instance of the Remote Filtering Client on a single Windows workstation to v6.3.3:



**Note**

This upgrade method does *not* preserve existing Remote Filtering Client configuration settings; communication information for Remote Filtering Server must be re-entered.

---

1. Run the v6.3.3 Websense installer on the Remote Filtering Client workstation to upgrade or install the Remote Filtering Client Pack:
  - If a previous version of the Remote Filtering Client Pack is installed on the machine, the Websense installer will detect it. Follow the onscreen instructions to upgrade it to v6.3.3.
  - If no previous version of the Remote Filtering Client Pack exists on the machine, follow the installation instructions in *Remote Filtering Client Pack*, page 131.
2. Navigate to the default installation location of  
C:\Program Files\Websense\bin\  
RemoteFilteringAgentPack\NO\_MSI\CPMClient.msi  
and double-click on the CPMClient.msi file to run the new Remote Filtering Client installer.
3. When the application detects an existing installation of Remote Filtering Client, it asks if you want to remove it. Click **Next** to continue.
4. When the **Remove the Program** dialog box appears, click **Remove**.
5. When the **InstallShield Wizard Completed** dialog box opens, click **Finish** to complete removal of the existing Remote Filtering Client.
6. Restart the machine.
7. Double-click on the CPMClient.msi file to run the Remote Filtering Client installer again.
8. Click **Next** to continue.
9. Re-enter the connection information for the primary Remote Filtering Server that this client uses for web filtering. If you are not certain of these values, you can view them in Websense files on the Remote Filtering Server machine:
  - a. Navigate to the `securewispproxy.ini` file, located in the `/bin` subdirectory in the Websense installation directory on the Remote Filtering Server machine.
  - b. Open the `securewispproxy.ini` file with a text editor to view the values of the following Remote Filtering Server parameters:
    - External IP address or host name: ProxyPublicAddress
    - External communication port: ProxyPort
    - Internal IP address or host name: ProxyIP
    - Internal communication port: HeartBeatPort

- c. If you do not remember the pass phrase you defined when installing the Remote Filtering Server, enter the encrypted key instead. The Websense software generates this key automatically by combining the pass phrase you defined with unpublished Websense keys. If you do not know the encrypted key, you can look it up if you have administrator rights on the Remote Filtering Server machine:
  - Navigate to the WSSEK.DAT file, located in the /bin subdirectory in the Websense installation directory on the Remote Filtering Server machine, and open it with a text editor to view the encrypted key.
10. If secondary and tertiary Remote Filtering Servers are being used, re-enter communication parameters for each of these servers as well.
11. Click **Next** to continue.
12. Click **Install** to begin installation.

When the installer is finished, a message appears advising you that the procedure was successful.
13. Click **Finish** to exit the installer.
14. If a message appears indicating that you must restart the machine, click **Yes** to restart now. Remote filtering will not function properly until the machine is restarted.

If no message appears, restarting the machine is not required.

## Upgrading Remote Filtering Client with a Third-Party Deployment Tool

This upgrade method allows you to deploy version 6.3.3 of the Remote Filtering Client to user workstations, while preserving the existing configuration settings.

To obtain the installer for version 6.3.3 of the Remote Filtering Client, you can:

- ◆ Upgrade an existing version of the Remote Filtering Client Pack to version 6.3.3 (see *Remote Filtering Client Pack*, page 50 for instructions).

-OR-

- ◆ Install version 6.3.3 of the Remote Filtering Client Pack on a Windows machine (see *Remote Filtering Client Pack*, page 131 for instructions).

If you selected the default installation path of C:\Program Files\WebSense, the installer is placed in the following location:

```
C:\Program Files\WebSense\bin\  
RemoteFilteringAgentPack\NO_MSI\CPMClient.msi
```

To deploy the new version of the Remote Filtering Client to Windows workstations, use this installer with a third-party deployment tool, such as Microsoft® Systems Management Server (SMS) or Novell® ZENworks®.

## Upgrade Syntax

The following is an example of the syntax to upgrade Remote Filtering Client using a third-party deployment tool. This command must be typed on a single line with no returns.

```
msiexec /i cpmclient.msi REINSTALL=ALL  
REINSTALLMODE=voums /qn
```

When the installer upgrades an installation of the Remote Filtering Client, the current configuration settings are used. If your remote filtering configuration *has not* changed, no additional parameters are necessary. However, if you have changed your configuration, you must include the appropriate parameters and new values in the command. For a complete list of command line parameters, see [Installing Remote Filtering Client with a Third-Party Deployment Tool](#), page 138.

If you are running a version of Websense Enterprise/Web Security Suite prior to v6.1, you must perform an intermediate upgrade first to bring your Websense Enterprise/Web Security Suite version level up to v6.1. For more information, see [Versions Supported](#), page 34.

## Converting a Stand-Alone System to an Integrated System

---

You can convert an existing Websense Stand-Alone Edition to a Websense system using Check Point FireWall-1 without losing any configuration

settings. The conversion process preserves such settings as port numbers and IP addresses.

## All Websense Filtering Components on the Same Machine

When all Websense Enterprise/Web Security Suite components are installed on the same machine, you can convert a Stand-Alone system to an integrated system by performing the following tasks:

**Task 1:** Upgrade to the v6.3.3 Stand-Alone Edition:

- If you have Websense v6.1 or higher Stand-Alone Edition installed, perform a direct upgrade to the v6.3.3 Stand-Alone Edition. This will preserve your configuration data and use the settings from your original system. Follow the procedures in [Upgrading to the New Stand-Alone Edition](#), page 57.
- If you have an earlier Websense stand-alone version installed, see v6.3.3 of the *Installation Guide for use with Stand-Alone Edition* for upgrade instructions.

**Task 2:** Restart the installation machine.

**Task 3:** Run the Websense installer again to convert the v6.3.1 Stand-Alone Edition to an integrated system using Check Point FireWall-1. Follow the procedures in [Converting to an Integrated System](#), page 66.

**Task 4:** Perform the tasks in [Chapter 5: Initial Setup](#).

**Task 5:** Configure FireWall-1 to communicate with the Websense software. For instructions, see [Chapter 7: Configuring FireWall-1 NG, NG with AI, and NGX](#).

## Distribute Websense Filtering Components

To convert your Websense Stand-Alone Edition to use Check Point FireWall-1 and move some Websense filtering components to other machines, perform the following tasks:

**Task 1:** Upgrade to the v6.3.3 Stand-Alone Edition:

- If you have Websense v6.1 or higher Stand-Alone Edition installed, perform a direct upgrade to the v6.3.3 Stand-Alone Edition. This will preserve your configuration data and use the settings from your original system. Follow the procedures in [Upgrading to the New Stand-Alone Edition](#), page 57.

- If you have an earlier Websense stand-alone version installed, see v6.3.3 of the *Installation Guide for use with Stand-Alone Edition* for upgrade instructions.

**Task 2:** Restart the installation machine.

**Task 3:** Run the Websense installer again and remove those components that you want to move to a different location in your network.



### **Warning**

Removing the Policy Server will delete all existing configuration settings.

---

**Task 4:** Run the Websense installer again to convert the v6.3.1 Stand-Alone Edition to an integrated system using Check Point FireWall-1. Follow the procedures in *Converting to an Integrated System*, page 66.

**Task 5:** Run the Websense installer on each machine in your network on which you want to install a separate component. Select a **Custom** installation when prompted and select the component you want to install. Separate installation procedures for individual components can be found in *Installing Websense Components Separately*, page 101.

**Task 6:** Perform the tasks in *Chapter 5: Initial Setup*.

**Task 7:** Configure FireWall-1 to communicate with the Websense software. For instructions, see *Chapter 7: Configuring FireWall-1 NG, NG with AI, and NGX*.



## Upgrading to the New Stand-Alone Edition

Your first task is to upgrade your v6.1 or higher Stand-Alone Edition to the v6.3.3 Stand-Alone Edition.



### Important

Websense services must be running when the upgrade process begins. The installer will stop and start these services as necessary during the upgrade. If these services have run uninterrupted for several months, however, the installer may not be able to stop them before the upgrade process times out.

To ensure the success of the upgrade, manually stop and restart all the Websense services before beginning the upgrade. To stop and start Websense services, follow the instructions in [Stopping or Starting Websense Services](#), page 185.

---

## Windows

The v6.3.3 Websense Enterprise/Web Security Suite installer can upgrade version 6.1 or higher of the Stand-Alone Edition.

1. Back up the following files before proceeding:

- `websense.ini`
- `eimserver.ini`
- `config.xml`



### Note

Before upgrading to a new version of Websense Enterprise/Web Security Suite, Websense, Inc., recommends that you perform a full system backup as a fallback strategy. This will allow you to restore your current production system with a minimum of downtime should you encounter any problems with the upgrade.

---

2. Close all Websense Managers anywhere in the network that connect to the Policy Server you are upgrading.

3. Log on to the installation machine with **domain** and **local** administrator privileges.
4. Close all applications and stop any antivirus software.



### Warning

Be sure to close the Windows Event Viewer, or the upgrade may fail.

---

5. Obtain a v6.3.3 Windows installer package for Websense Enterprise/Web Security Suite:

**Web download:** To download an installer package, go to [www.websense.com](http://www.websense.com), and then navigate to the Downloads page.

- a. Choose the dynamic (online) or full (offline) installer package, the operating system, and the language.



### Note

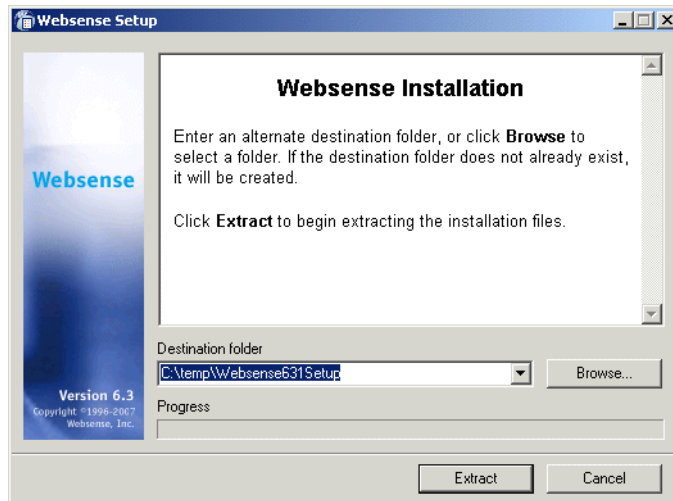
The **Dynamic** installer is an **online** installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.

The **Full** installer is a complete **offline** installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install the Websense Enterprise/Web Security Suite components. Use this package if you experience difficulties with the online installer.

---

- b. Download the selected installer package to a folder on the installation machine, and double-click to extract the installer files.

A screen displays instructions for extracting the setup program.



Websense Installer File Extraction

6. If you do not want to accept the default location, click **Browse** to select a destination folder, or type in a path.  
If the path you enter does not exist, the installer will create it for you.



### Important

Do not extract the installer files to a folder on your desktop. This may prevent the Real-Time Analyzer from receiving the IP address of the Policy Server machine. Accept the default location of `C:\temp` or select another appropriate folder.

---

7. Click **Extract** to begin decompressing the files.
  - If Websense installation files already exist in that location, you may choose to overwrite the existing files.
  - A progress bar shows the status of the extraction, and the view pane scrolls a list of the files as they are decompressed.
  - `Setup.exe` runs automatically after the files are decompressed.
8. Follow the onscreen instructions and click **Next** to advance through the welcome screen and the subscription agreement.

The installer detects the Websense components from your earlier version and asks how you want to proceed. You can upgrade the current system or exit the installer.

9. Select **Upgrade** and click **Next**.

A list of currently running Websense services from the earlier version appears. A message explains that the installer must stop these services before the installation can proceed.

10. Click **Next** to continue.

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation will continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary screen appears, listing the installation path, installation size, and the components that will be installed.

11. Click **Next** to begin the upgrade.

- The Download Manager copies the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.
- If you are using the Apache HTTP Server, you must restart it before using the Real-Time Analyzer on your upgraded system. The installer asks if you want to restart Apache now or wait until later. Select **Yes** or **No** and click **Next** to continue.

The installer asks if you want to download the Websense Master Database now or at a later time using Websense Manager.



---

### Warning

During upgrade, the installer removes the existing Master Database. Websense filtering cannot resume until the new Master Database has been successfully downloaded, decompressed, and loaded. This may take a few minutes or more than 60 minutes, depending on factors such as internet connection speed, bandwidth, available memory, and free disk space.

---

12. Select a Master Database download option and click **Next**.

If you have chosen to download the Master Database now, a progress bar appears. The database must first be downloaded from the internet, and then decompressed and loaded into local memory. Downloading the database from the internet can take a few minutes or more than 30 minutes, depending on factors such as internet connectivity, bandwidth, time of day, and your location relative to the download server. Decompressing and loading the database can take a few minutes or more than 30 minutes, depending on factors such as available memory, free disk space, and server process utilization.

When the database has finished loading, a message appears advising you of the status of the download. Click **Next** to continue.

13. When a message announcing successful completion of the installation is displayed:

- If you chose a non-English language installer, click **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions to update Websense components with text in the selected language.
- If you chose an English language installer:
  - If Websense Manager was not upgraded, no further action is required and you can click **Finish** to exit the installer.

- If Websense Manager was upgraded, click **Next** to continue. The installer displays a screen asking if you want to launch Websense Manager. If you do not want to launch Manager, clear the checkbox. Click **Finish** to exit the installer.

14. If you stopped your antivirus software, be sure to start it again.

## Solaris or Linux

The v6.3.3 Websense Enterprise/Web Security Suite installer can upgrade version 6.1 or higher of the Stand-Alone Edition.

1. Back up the following files before proceeding:
  - `websense.ini`
  - `eimserver.ini`
  - `config.xml`



### Note

Before upgrading to a new version of Websense Enterprise/Web Security Suite, Websense, Inc., recommends that you perform a full system backup as a fallback strategy. This will allow you to restore your current production system with a minimum of downtime should you encounter any problems with the upgrade.

---

2. Close all Websense Managers anywhere in the network that connect to the Policy Server you are upgrading.
3. Log on to the installation machine as the **root** user.
4. Close all applications and stop any antivirus software.
5. Create a setup directory for the installer files.  
For example: `/root/Websense_setup`
6. Obtain a v6.3.3 Solaris or Linux installer package for Websense Enterprise/Web Security Suite:

**Web download:** To download an installer package, go to [www.websense.com](http://www.websense.com), and then navigate to the Downloads page.

- a. Choose the dynamic (online) or full (offline) installer package, the operating system, and the language.



### Note

The **Dynamic** installer is an **online** installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.

The **Full** installer is a complete **offline** installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install the Websense Enterprise/Web Security Suite components. Use this package if you experience difficulties with the online installer.

- b. Save the selected installer package to the setup directory on the installation machine.
7. In the setup directory, enter the following command to unzip the file:  

```
gunzip <download file name>
```

 For example: `gunzip Websense62Setup_Slr.tar.gz`
  8. Expand the file into its components with the following command:  

```
tar xvf <unzipped file name>
```

 For example: `tar xvf Websense62Setup_Slr.tar`  
 This places the following files into the setup directory:

File	Description
install.sh	Installation program
Setup	Archive file containing related installation files and documents.
Documentation	Release Notes: An HTML file containing release notes and last minute information about the Websense software. Read this file with any supported browser.

9. Run the installation program from the setup directory with the following command:

```
./install.sh
```

To run the GUI version of the installer, use the following command:

```
./install.sh -g
```

If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.

10. Follow the onscreen instructions through the subscription agreement.
11. Follow the upgrade sequence:
  - **Websense upgrade:** The installer detects the earlier version of Websense components and gives you the choice of upgrading the existing installation or exiting Setup. Be sure to close any Websense Managers connected to the Policy Server being upgraded before continuing. Select **Upgrade** and continue.
  - **Stopping Websense services:** A list of currently running Websense services from the earlier version appears. A message explains that the installer must stop these services before the upgrade can proceed. Select **Next** to continue.
  - **System requirements check:** The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.
    - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
    - If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.
  - **Installation summary:** A summary list appears, showing the installation path, file sizes, and the components that will be upgraded.
12. Select **Next** to begin the upgrade.

The Download Manager indicates the progress of the file download from the Websense website. After the files are downloaded, the installer stops all Websense services.

An installation progress bar appears and the Websense services are restarted.



- **Master Database Download:** The installer asks if you want to download the Websense Master Database now or at a later time using Websense Manager. Select a database download option and then select **Next** to continue.



### Warning

During upgrade, the installer removes the existing Master Database. Websense filtering cannot resume until the new Master Database has been successfully downloaded, decompressed, and loaded. This may take a few minutes or more than 60 minutes, depending on factors such as internet connection speed, bandwidth, available memory, and free disk space.

---

- If you have chosen to download the Master Database now, the download begins. The database must first be downloaded from the internet, and then decompressed and loaded into local memory. Downloading the database from the internet can take a few minutes or more than 30 minutes, depending on factors such as internet connectivity, bandwidth, time of day, and your location relative to the download server. Decompressing and loading the database can take a few minutes or more than 30 minutes, depending on factors such as available memory, free disk space, and server process utilization.
- When the database has finished loading, a message appears advising you of the status of the download. Select **Next** to continue.
13. When a message announcing successful completion of the installation is displayed:
    - If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions to update Websense components with text in the selected language.
    - If you chose an English language installer:
      - If you are installing in command line mode, select **Finish** to exit the installer.
      - If you are installing in GUI mode, select **Next** to continue. The installer asks if you want to start Websense Manager. Make a choice and select **Finish** to exit the installer.
  14. If you stopped your antivirus software, be sure to start it again.

## Converting to an Integrated System

Once you have upgraded your existing Stand-Alone Edition to the v6.3.1 Stand-Alone Edition, you are ready to convert to a system that integrates with Check Point FireWall-1.

### Windows

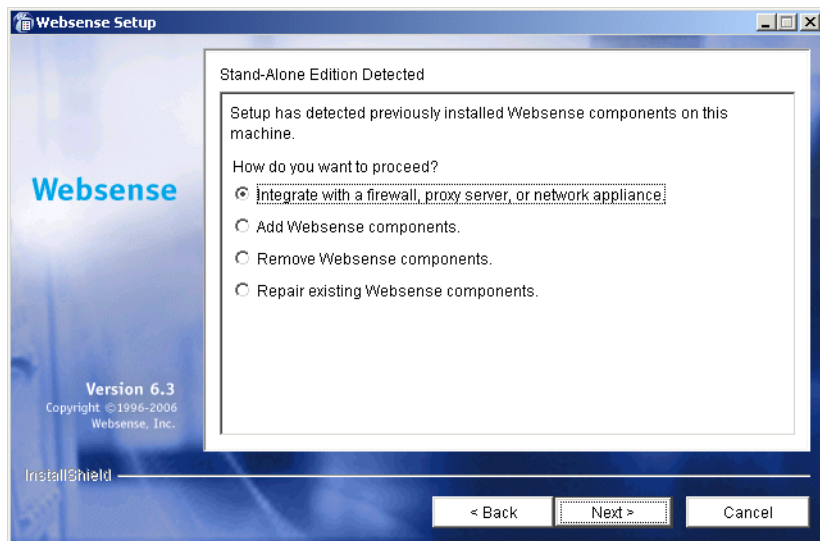
To convert a Windows v6.3.1 Websense Stand-Alone Edition to a v6.3.1 Websense system integrated with Check Point FireWall-1:

1. Back up the following files before proceeding:
  - `websense.ini`
  - `eimserver.ini`
  - `config.xml`
2. Close all Websense Managers anywhere in the network that connect to the Policy Server you are upgrading.
3. Log on to the installation machine with **domain** and **local** administrator privileges.
4. Close all applications and stop any antivirus software.
5. Run the v6.3.3 Websense Enterprise/Web Security Suite installer for Windows.

To do this, double-click on `Setup.exe` in the local directory where you unpacked the installer when you upgraded to v6.3.3 of the Stand-Alone Edition in *Upgrading to the New Stand-Alone Edition*, page 57.

6. Click **Next** in the welcome screen.

The installer detects the Websense Stand-Alone Edition and asks how you want to proceed.



Stand-Alone Edition Detected

7. Select **Integrate with a firewall, proxy server, or network appliance** and click **Next**.

A message explains that the installer must stop the Filtering Service before the upgrade can proceed.

8. Click **Next** to continue.

A dialog box appears listing the supported integration types.

9. Select **Check Point FireWall-1** and click **Next**.

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, warnings are displayed in separate screens.

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation will continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary screen appears, listing the installation path, installation size, and the components that will be installed.

10. Click **Next** to begin installation.

The Download Manager progress bar appears, tracking the progress of the installer download. When the appropriate files have been downloaded, the installer stops the Websense services and begins installation.

The installer asks if you want to download the Websense Master Database now or at a later time using Websense Manager.

11. Select a database download option and click **Next**.

If you have chosen to download the Master Database now, a progress bar appears. The database must first be downloaded from the internet, and then decompressed and loaded into local memory. Downloading the database from the internet can take a few minutes or more than 30 minutes, depending on factors such as internet connectivity, bandwidth, time of day, and your location relative to the download server. Decompressing and loading the database can take a few minutes or more than 30 minutes, depending on factors such as available memory, free disk space, and server process utilization.

When the database has finished loading, a message appears advising you of the status of the download.

12. Click **Next** to continue.

A message appears advising you that the installation was successful.

13. Click **Next** to continue.

If you chose a non-English language installer, the Language Pack Installation screen appears, advising you that the Language Pack cannot be installed due to an impending reboot. Click **Next** to continue.

14. When a dialog box appears advising you that the machine must be restarted to complete the installation, select **Yes** to restart the machine.

15. Click **Finish** to exit the installer and restart the machine.

16. If you used a non-English language installer, run the Language Pack installer now to convert Websense software to your language:

- a. Go to the setup folder where you unpacked the Websense installer, and double-click on `SetupLanguagePack.exe`.
- b. Follow the onscreen instructions to complete installation of the Language Pack.

17. If you stopped your antivirus software, be sure to start it again.

## Solaris or Linux

To convert a Solaris or Linux v6.3.1 Websense Stand-Alone Edition to a v6.3.1 Websense system integrated with Check Point FireWall-1:

1. Back up the following files before proceeding:
  - `websense.ini`
  - `eimserver.ini`
  - `config.xml`
2. Close all Websense Managers anywhere in the network that connect to the Policy Server you are upgrading.
3. Log on to the installation machine as the **root** user.
4. Close all applications and stop any antivirus software.
5. Run the Websense installer from the directory where you unpacked it using the following command:

```
./install.sh
```

To run the GUI version of the installer, use the following command:

```
./install.sh -g
```

If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.

6. Make the following selections:
  - **Stand-Alone Edition Detected:** The installer detects the presence of the Websense Stand-Alone Edition and asks what you want to do. Select **Integrate with a firewall, proxy server, or network appliance** and continue.
  - **Stopping Websense services:** A message explains that the installer must stop the Filtering Service before the installation can proceed. Select **Next** to continue.
  - **Integration product:** Select **Check Point FireWall-1** from the list of supported integration types.
  - **System requirements check:** The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.
    - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.
  - **Installation summary:** A summary list appears, showing the installation path, file sizes, and the components that will be installed.
7. Select **Next** to begin installation.

The Download Manager copies the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.

The installer asks if you want to download the Websense Master Database now or at a later time using Websense Manager.
  8. Select a database download option and click **Next**.

If you have chosen to download the Master Database now, a progress bar appears. The database must first be downloaded from the internet, and then decompressed and loaded into local memory. Downloading the database from the internet can take a few minutes or more than 30 minutes, depending on factors such as internet connectivity, bandwidth, time of day, and your location relative to the download server. Decompressing and loading the database can take a few minutes or more than 30 minutes, depending on factors such as available memory, free disk space, and server process utilization.

When the database has finished loading, a message appears advising you of the status of the download.
  9. Click **Next** to continue.
  10. When a message announcing successful completion of the installation is displayed:
    - If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions to update Websense components with text in the selected language.
    - If you chose an English language installer, select **Finish** to exit the installer.
  11. If you stopped your antivirus software, be sure to start it again.

## Updating the Websense Resource Object

---

After upgrading Websense software, you must reselect certain values for the Websense Resource Object in FireWall-1, in order to verify that FireWall-1 is communicating with the Websense UFP Server properly.

1. Select **Manage > Resources**.  
The **Resources** dialog box appears.
2. Select the Websense Resource Object, and then click the **Edit** button.
3. Navigate to the appropriate tab.
  - *FireWall-1 NG Policy Editor*: Go to the **Match** tab in the **URI Resource Properties** dialog box.
  - *FireWall-1 NG with AI, FireWall-1 NGX SmartDashboard™*: Go to the **Match** tab in the **URI Resource Properties** dialog box.
4. Reselect the object created for the Websense UFP Server from the **UFP Server** drop-down list.
5. Uncheck and then recheck the correct category (**Blocked** or **Not Blocked**) in the **Categories** list.
6. Select **Policy > Install** to reinstall the policy on the firewall.

## Migrating Between FireWall-1 Versions After an Upgrade

---

If you plan to upgrade your Check Point FireWall-1 installation (from FireWall-1 NG to FireWall-1 NGX, for example), you may do so after you upgrade to Websense Enterprise or Web Security Suite v6.3.1 without any additional modifications to your Websense system. See your Check Point documentation for information about upgrading FireWall-1.

See *Chapter 7: Configuring FireWall-1 NG, NG with AI, and NGX* for the necessary configuration procedures to ensure that your new version of FireWall-1 can communicate with Websense Enterprise or Web Security Suite v6.3.1.

## Changing IP Addresses of Installed Components

---

Websense filtering software handles most IP address changes automatically, without any interruption in internet filtering. Changes to the IP address of the machine running the Policy Server result in notification of the change being broadcast to Websense components on other machines. In some cases, however, services need to be restarted or configurations updated after changing an IP address. For a full discussion of the IP address change process, see the *Administrator's Guide* for Websense Enterprise/Web Security Suite.



# Installing Websense Enterprise/ Websense Web Security Suite

This chapter contains instructions for a new installation of Websense Enterprise/Web Security Suite components. In addition to installation procedures, instructions are provided for modifying an installation, including adding, removing, and repairing installed components.

## Websense Installers

---

Separate Websense installers are available for the Windows, Solaris, and Linux operating systems. There is one Websense product installer for each operating system:

### **Websense Enterprise/Websense Web Security Suite**

For information about using the product features after you have completed installation, see the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

All Websense installers are available in English and nine other language versions. See [Non-English Language Versions, page 73](#) if you plan to use your Websense software in a non-English language environment.

## Non-English Language Versions

The Websense Enterprise/Web Security Suite v6.3.3 installer package is available for the following languages:

Language	Code
Chinese (Simplified)	zh_CN
Chinese (Traditional)	zh_TW
English	en

Language	Code
French	fr
German	de
Italian	it
Japanese	ja
Korean	ko
Portuguese (Brazil)	pt_BR
Spanish	es

Go to [www.websense.com](http://www.websense.com), navigate to the Downloads page, and then select an installer package for the desired language.



**Important**

All Websense components in a Websense installation must be in the same language.

---

Each non-English installer package includes a Language Pack that converts your Websense system to that language. The Language Pack installer launches automatically following completion of the main Websense installer. Simply follow the onscreen instructions to complete the installation of the Language Pack.



**Note**

**Installer Language:** The Japanese version of the Websense installer and Language Pack installer are in Japanese. The Websense installer and Language Pack installer for all other languages are in English.

---

The Language Pack makes the following modifications to a Websense Enterprise/Web Security Suite system:

- ◆ Localized block page files are copied into a new directory created for the selected non-English language on the installation machine. The directory name is the language code shown in the preceding table.

- ◆ The Websense configuration file (`config.xml`) is edited to localize certain data strings such as warnings and error messages.
- ◆ Websense category names are updated with localized versions.
- ◆ Alert messages for Websense Administrators are updated with localized versions.
- ◆ The Reporting Tools Portal and Real-Time Analyzer are updated with localized versions.
- ◆ *Japanese only*: The Websense Manager user interface is converted to Japanese.



### Note

For information about the modifications that Language Pack makes to the Websense Reporting components, see the *Reporting Installation Guide* for Websense Enterprise/Web Security Suite.

For information about the modifications that Language Pack makes to Client Policy Manager components, see the *Installation Guide* for Websense Client Policy Manager.

---

## Before Installing

---

Read the following information before installing Websense Enterprise/Web Security Suite.

- ◆ **Do not install Websense components on the FireWall-1 machine:** Installing Websense components on the same machine as FireWall-1 is *not* recommended by either Check Point or Websense, Inc.  
The exception is installing on a blade server that has separate processors to accommodate Websense components and the Firewall-1 software.
- ◆ **Reporting:** To properly generate reports, you must use the same version of Websense filtering software and Websense Reporting Tools.



### Important

Install all Websense Enterprise/Web Security Suite components *before* installing Websense Reporting components.

---

For information about installing Reporting components, see the *Reporting Installation Guide* for Websense Enterprise/Web Security Suite.

- ◆ **Deployment:** You can install the main Websense filtering components together on the same machine or distribute them on separate machines, depending upon the available operating systems and the size of your network. If you plan to distribute your Websense components on separate machines in your network, run the installer on each machine and select the **Custom** installation option. For instructions, see [Installing Websense Components Separately](#), page 101.

You can install Websense components on separate machines that do not have the same operating system. For example, you can install Websense Manager on a Windows machine and use it to configure a Policy Server running on a Linux machine. As long as each Websense component is supported on the operating system of the machine where it is installed, the components will work together. A list of system requirements for each Websense component can be found in the *Deployment Guide* for Websense Enterprise/Web Security Suite.

Be sure to read the *Deployment Guide* for Websense Enterprise/Web Security Suite before beginning installation to determine the appropriate deployment of Websense components in your network. The *Deployment Guide* also contains system requirements, including the supported operating systems for each Websense component and the supported versions of your integration product.

- ◆ **Computer clock synchronization:** If you are distributing Websense components in your network, synchronize the clocks on all machines on which a Websense component will be installed.
- ◆ **Remote filtering:** To install the optional Remote Filtering components that allow filtering of workstations located outside the network firewall, you must run the Websense installer and select a **Custom** installation. For information, see [Installing Websense Components Separately](#), page 101.
- ◆ **Network Agent:** Network Agent is included as part of a Typical installation. The machine on which Network Agent is installed must be deployed so that Network Agent is able to monitor all requests sent from user workstations to the internet, as well as all replies from the internet to the requesting workstations. If you install Network Agent on a machine that cannot monitor the targeted traffic, Network Agent features such as Protocol Management, Bandwidth Optimizer, and IM Attachment Manager will not work correctly. For more information about positioning the

Network Agent machine in your network, see the Network Agent chapter in the *Deployment Guide* for Websense Enterprise/Web Security Suite.



### Important

*Do not* install Network Agent on a machine running any type of firewall. Network Agent uses a packet-capturing utility which may not work properly when installed on a firewall machine. The only exception is a blade server or appliance that has separate processors or virtual processors to accommodate Network Agent and the firewall software.

- ◆ **Network Interface Card (NIC):** The NIC that you designate for use by Network Agent during installation must support *promiscuous* mode. Promiscuous mode allows a NIC to listen to IP addresses other than its own. (Contact the manufacturer of your card to see if it supports promiscuous mode.) If the card supports promiscuous mode, it will be set to that mode by the Websense installer during installation.



### Note

If you install Network Agent on a machine with multiple NICs, you can configure Network Agent after installation to use more than one NIC. See [Configuring Network Agent to use Multiple NICs, page 204](#) for more information.

After installation, you can run the Traffic Visibility Tool to test whether the selected NIC can see the appropriate user internet traffic. See [Testing Visibility of Internet Traffic to Network Agent, page 204](#)

- ◆ **Web server:** To install Real-Time Analyzer (RTA) you must have either Microsoft IIS or Apache HTTP Server installed. If neither supported web server is detected, the installer gives you the option to install the Apache HTTP Server or continue the installation without installing RTA.
- ◆ **Internet access:** For the Websense Master Database download to occur during installation, the machine running the Websense Filtering Service must have internet access to the download servers at the following URLs:
  - download.websense.com
  - ddsdom.websense.com
  - ddsint.websense.com

- portal.websense.com
- my.websense.com

Make sure that these addresses are permitted by all firewalls, proxy servers, routers, or host files that control the URLs that Filtering Service can access.

- ◆ **Remote Control Utilities:** Installation of Websense Enterprise/Web Security Suite using a remote control utility such as Terminal Services is not supported.
- ◆ **Enabling Java interfaces:** If you are installing any Websense components on a Windows 2000 Server machine, you must install DirectX to launch the Java-based GUI installer. If DirectX is not present, you can only install Websense components in the console mode. To enable the console installer in Windows 2000, see the procedure in the troubleshooting topic *Websense splash screen is displayed, but installer does not launch on Windows 2000*, page 262.

If you have performed a console installation on a Windows 2000 Server machine without DirectX, you must install Websense Manager on a Solaris machine or on a Windows or Linux machine capable of displaying a Java interface.

## Typical Websense Installation

---

This section provides separate instructions for installing Websense Enterprise/Web Security Suite components on each operating system.

### Windows

Follow the procedures in this section to install Websense Enterprise/Web Security Suite on a Windows machine. These procedures are for a **Typical** installation, in which the main Websense filtering components are installed on the same machine, separate from FireWall-1.

If you plan to distribute the main Websense components on separate machines in your network, you must install the Policy Server first. Only Websense Manager can be installed before the Policy Server has been successfully installed. To install components separately, run the Websense installer on each machine and select a **Custom** installation. For instructions to install Websense components separately, see *Installing Websense Components Separately*, page 101.

If you decide to change the location of a Websense component, add a component, or remove a component, run the Websense installer again on the machine you want to modify and select the appropriate option. The installer detects the presence of Websense components and offers you options for modifying your installation. For information about adding or removing Websense components, see [Adding Components, page 163](#) and [Removing Components, page 173](#).

To install Websense Enterprise or Web Security Suite on a Windows machine not running Check Point FireWall-1:

1. Log on to the installation machine with **domain** and **local** administrator privileges.

If you are installing User Service and DC Agent, this will assure that they have administrator privileges on the domain.



### Important

User Service and DC Agent must have administrator privileges on the network to retrieve user login information from the domain controller. Without this information, Websense software cannot filter by users and groups. If you cannot install these components with such privileges, you can configure domain administrator privileges for these services after installation. For instructions, see [Configure Domain Administrator Privileges, page 207](#).

---

2. Close all applications and stop any antivirus software.
3. Obtain an installer package for Websense Enterprise/Web Security Suite:

**Web download:** To download an installer package, go to [www.websense.com](http://www.websense.com), and then navigate to the Downloads page.

- a. Choose the dynamic (online) or full (offline) installer package, the operating system, and the language.



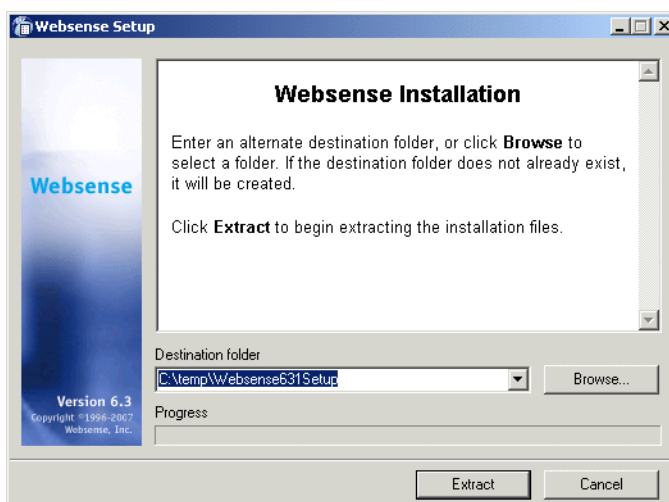
### Note

The **Dynamic** installer is an **online** installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.

The **Full** installer is a complete **offline** installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install the Websense Enterprise/Web Security Suite components. Use this package if you experience difficulties with the online installer.

- b. Download the selected installer package to a folder on the installation machine, and double-click to extract the installer files.

A screen displays instructions for extracting the setup program.



Websense Installer File Extraction

1. If you do not want to accept the default location, click **Browse** to select a destination folder, or type in a path.



If the path you enter does not exist, the installer will create it for you.



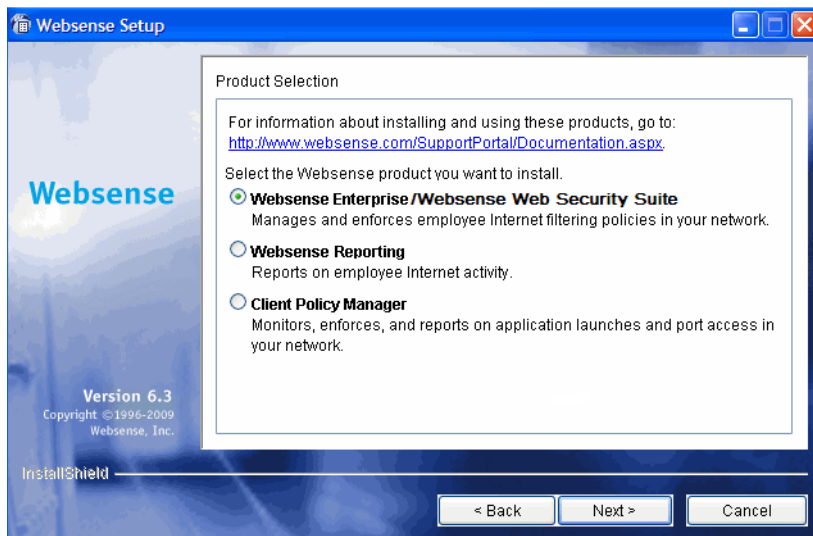
### Important

Do not extract the installer files to a folder on your desktop. This may prevent the Real-Time Analyzer from receiving the IP address of the Policy Server machine. Accept the default location of `C:\temp` or select another appropriate folder.

---

2. Click **Extract** to begin decompressing the files.
  - If Websense installation files already exist in that location, you may choose to overwrite the existing files.
  - A progress bar shows the status of the extraction, and the view pane scrolls a list of the files as they are decompressed.
  - `Setup.exe` runs automatically after the files are decompressed.
3. Click **Next** in the welcome screen and follow the onscreen instructions through the subscription agreement.

4. In the Product Selection screen, select the product to install and click **Next**:
  - *Websense Enterprise/Web Security Suite installer*: Select **Websense Enterprise/Websense Web Security Suite**.



Websense Product Selection

5. You are offered a choice of two setup types:
  - **Typical**: Installs Filtering Service, Policy Server, Real-Time Analyzer, Websense Manager, User Service, Usage Monitor, and Network Agent together on the same machine. The installer gives you the option of installing the following transparent identification agents: DC Agent, eDirectory Agent, Logon Agent, and RADIUS Agent.
  - **Custom**: Allows you to choose individual Websense components to install. Use this option to install Websense components on different machines in your network. For more information, see *Installing Websense Components Separately*, page 101.
6. Select **Typical** and click **Next**.

If the installation machine is multihomed, all enabled network interface cards (NICs) with an IP address appear in a list.
7. Select the IP address of the card to use for Websense communications and click **Next**.

The installer asks if you want to run Websense software in the stand-alone filtering mode, or integrate it with a firewall, proxy server, cache, or network appliance.

8. Select **Integrated** and click **Next**.

A dialog box appears listing the supported integration types.

9. Select **Check Point FireWall-1** and click **Next**.
10. The installer automatically assigns default port numbers to the Policy Server (55806) and the Filtering Service (15868). If either of these default ports is in use, the installer asks you to enter an alternate port. Enter an unused port number between 1024 and 65535 and click **Next** to continue.



#### Note

Record the port numbers if you change them from the defaults. You will need them when installing other Websense components.

---

The installer displays the **Websense Subscription Key** dialog box.

11. Choose from the following subscription key options:
  - **I have a Websense subscription key:** If you have a valid subscription key, select this option and enter your key. You will be given the option to download the Websense Master Database during installation. This will enable the Websense software to begin filtering immediately.
  - **I do not wish to use a key at this time:** Select this option to continue the installation without entering a key. You will not be given the option to download the Websense Master Database during installation. You can download the Master Database after installation by entering a valid key in Websense Manager. For instructions, see *Subscription Key and Master Database Download*, page 190.

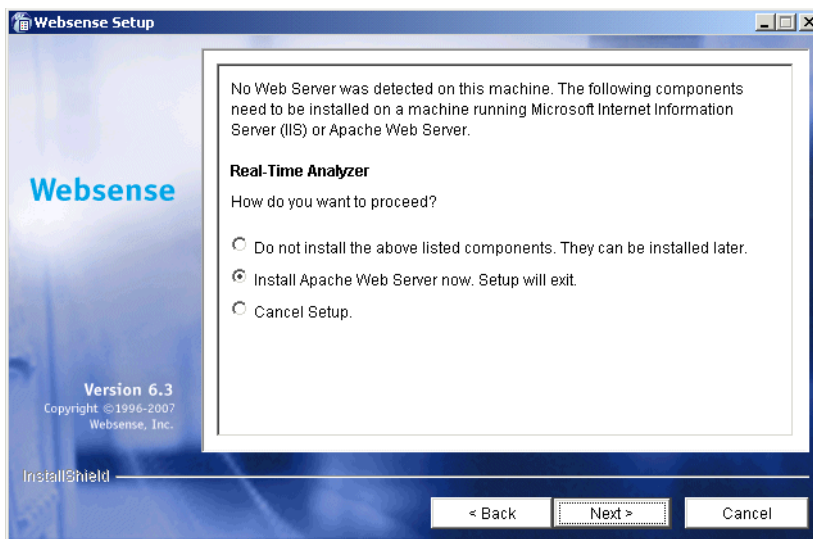
To request a 30-day evaluation key, go to:

[www.websense.com/evaluations](http://www.websense.com/evaluations).

12. Click **Next** to continue.

The installer checks your system for a supported web server (Apache HTTP Server or IIS) for the Real-Time Analyzer and takes the following action:

- If both supported web servers are detected, a dialog box appears asking you to choose one server for the RTA instance.
- If one of the supported servers is detected, the installer continues. No notification appears.
- If neither supported web server is detected, the installer gives you the option to install the Apache HTTP Server or continue the installation without installing RTA.



Web Server for Real-Time Analyzer

If you select the Apache HTTP Server installation option, the Websense installer starts the Apache installer and exits without installing any Websense components. You must restart your computer after installing the Apache HTTP Server and run the Websense installer again to install Websense.



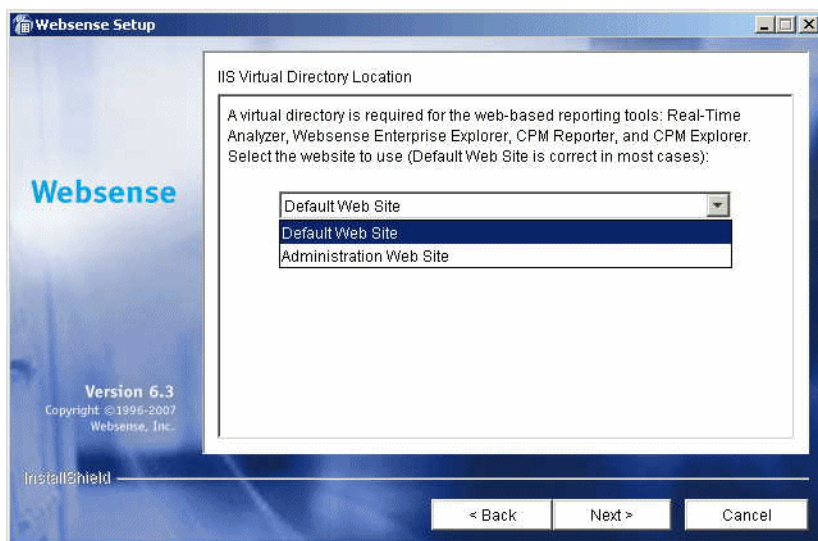
**Note**

Apache HTTP Server documentation is installed in HTML format in the `docs/manual/` directory. It is also available at: <http://httpd.apache.org/docs/2.0/>.

---

13. Select a web server installation option and click **Next** to continue.

If you are installing the Real-Time Analyzer and are using IIS as your web server, you are prompted to select the name of the website in the IIS Manager under which the installer should create a virtual directory. The default value is **Default Web Site**, which is correct in most instances.



Virtual Directory Selection

14. If you have renamed the default website in the IIS Manager or are using a language version of Windows other than English, select the proper website from the names in the drop-down list, and then click **Next** to continue.

15. Click **Next** to continue.

The installer warns you that Network Agent cannot function properly on a machine that is being used as a firewall. (The exception is a blade server that has separate processors to accommodate Websense software and the Firewall-1 software.)

16. Select **Yes** or **No** and click **Next** to continue:
  - If the installation machine is *not* being used as a firewall, select **Yes** to install Network Agent.
  - If you are installing on a firewall machine—for example, the FireWall-1 machine—select **No**. Installation of the rest of the Websense components will continue, but Network Agent will not be installed. Install Network Agent later on a machine that is not running a firewall.

If you are installing Network Agent, a screen appears asking you to select the network interface card (NIC) that you want Network Agent to use for capturing traffic. All network interface cards enabled in the machine appear in a list.

17. If the machine has multiple NICs, select the one that has visibility into the internet traffic you want Network Agent to filter.



#### Note

After installation, you can run the Traffic Visibility Tool to test whether the selected NIC can see the appropriate user internet traffic. See [Testing Visibility of Internet Traffic to Network Agent](#), page 204.

---

18. Click **Next** to continue.

If you are installing Network Agent, a screen appears asking if you want to allow Websense, Inc., to gather information about the use of Websense-defined protocols. Information will be used in the development of protocol filtering.



#### Note

Network Agent never sends Websense, Inc., any information that would identify specific users, no matter which Network Agent feedback option is selected.

---

19. Select a Network Agent feedback option and click **Next** to continue.

The installer asks you to select an initial filtering option.

- **Yes:** Configures Websense software to filter internet traffic immediately after installation, based on a predefined default policy.
- **No:** Configures Websense software to monitor internet traffic only, while permitting all internet requests. Select this option if you prefer to evaluate your network traffic before applying internet filtering.

20. Select an initial filtering option and click **Next** to continue.

The installer displays the **Transparent User Identification** screen, allowing you to select how Websense software will identify users:

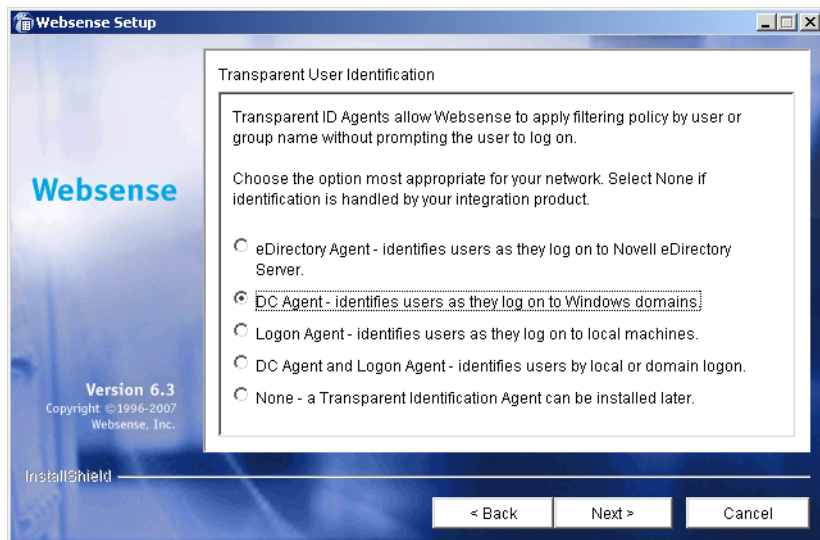
- **eDirectory Agent:** Select this option to install eDirectory Agent to authenticate users transparently with Novell eDirectory Service.

- **DC Agent:** Select this option to install DC Agent to authenticate users transparently with a Windows-based directory service.
- **Logon Agent:** Select this option to install Logon Agent to authenticate users transparently when they log on to the domain. Logon Agent receives its user information from an application called `LogonApp.exe` that must be run by a logon script in your network. For instructions, see *Creating and Running the Script for Logon Agent*, page 196.
- **DC Agent and Logon Agent:** Select this option to install both DC Agent and Logon Agent to authenticate users transparently. This can increase the accuracy of user identification in some networks.
- **None:** This option does not install a Websense transparent identification agent. Select this option if you plan to configure authentication of users through Check Point FireWall-1.



**Note**

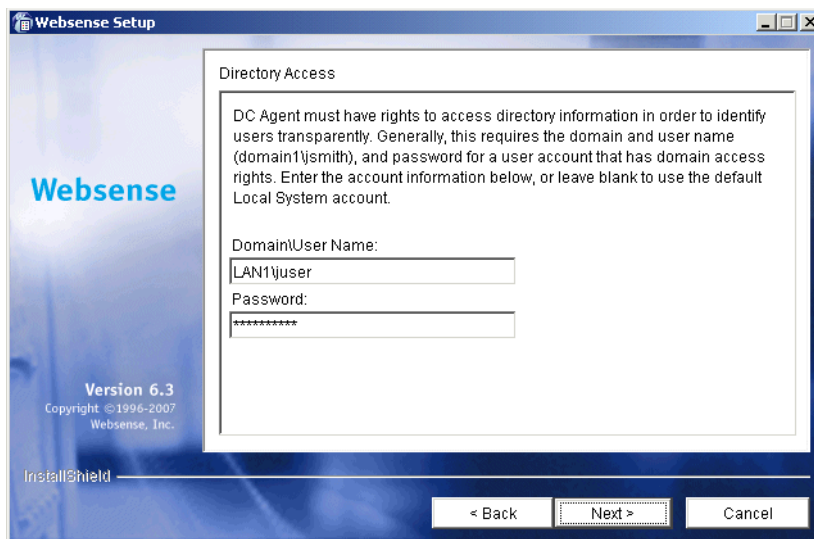
You can configure manual authentication in Websense Manager after installation. For instructions, see the *Administrator's Guide* for Websense Enterprise/Web Security Suite.



Transparent User Identification Option

21. Select a transparent identification method and click **Next** to continue.  
The installer displays the **RADIUS Agent** screen.
22. If you have remote users who are authenticated by a RADIUS server, you can select **Yes** to install the optional Websense RADIUS Agent. RADIUS Agent will allow the Websense software to transparently identify these users.
23. Click **Next** to continue.

If you selected DC Agent for installation, you are asked to provide a user name and a password with administrative privileges on the domain. DC Agent needs access to directory information to be able to identify users transparently.



Directory Access for DC Agent

24. Enter the domain and user name, followed by the network password for an account with domain privileges, and click **Next** to continue.



**Note**

If you cannot install DC Agent with the appropriate privileges, you can configure domain administrator privileges for it after installation. For instructions, see [Configure Domain Administrator Privileges, page 207](#).

---



A dialog box appears, asking you to select an installation folder for the Websense components.

25. Accept the default path (C:\Program Files\Websense) or click **Browse** to locate another installation folder, and then click **Next** to continue.

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary list appears, showing the installation path, the installation size, and the components that will be installed.

26. Click **Next** to start the installation.

- The appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.
- If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

If you provided the installer with a valid subscription key when prompted, you are asked if you want to download the Websense Master Database now or at a later time using Websense Manager.

27. Select a database download option and click **Next**.

If you have chosen to download the Master Database now, a progress bar appears. The database must first be downloaded from the internet, and then decompressed and loaded into local memory. Downloading the database from the internet can take a few minutes or more than 30 minutes, depending on factors such as internet connectivity, bandwidth, time of day, and your location relative to the download server.

Decompressing and loading the database can take a few minutes or more than 30 minutes, depending on factors such as available memory, free disk space, and server process utilization.

When the database has finished loading, a message appears advising you of the status of the download.

28. Click **Next** to continue.

A message announcing the successful completion of the installation is displayed.

29. Click **Next** to continue.

- If you chose a non-English language installer, the Websense Language Pack installer starts. Click **Next** in the welcome screen and follow the onscreen instructions to update Websense components with text in the language you selected.
- If you chose an English language installer, a screen appears asking if you want to launch Websense Manager. If you do not want to launch Manager, clear the checkbox. Click **Finish** to exit the installer.



#### **Note**

Before you can access Real-Time Analyzer and other Websense Reporting Tools, you must first log on to Websense Manager and configure user permissions. For more information, see the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

---

30. If you stopped your antivirus software, be sure to start it again.
31. See [Chapter 5: Initial Setup](#) to perform post-installation tasks.

32. See [Chapter 6: Using FireWall-1 with Websense Software](#) to learn about how Websense software works with FireWall-1, then follow the instructions in [Chapter 7: Configuring FireWall-1 NG, NG with AI, and NGX](#) to define the necessary objects and rules to support Websense filtering.



#### Note

If you decide to change the location of a Websense component, add a component, or repair a component, run the Websense installer again on the machine you want to modify and select the appropriate option. The installer detects the presence of Websense components and offers you options for modifying your installation. For instructions, see [Modifying an Installation](#), page 163.

---

## Solaris or Linux

Follow the procedures in this section to install Websense Enterprise/Web Security Suite on a Solaris or Linux machine. These procedures are for a **Typical** installation, in which the main Websense filtering components are installed on the same machine.

If you plan to distribute the main Websense components on separate machines in your network, you must install Policy Server first. Only Websense Manager can be installed before Policy Server has been successfully installed. To install components separately, run the Websense installer on each machine and select a **Custom** installation. For instructions to install Websense components separately, see [Installing Websense Components Separately](#), page 101.

If you decide to change the location of a Websense component, add a component, or remove a component, run the Websense installer again on the machine you want to modify and select the appropriate option. The installer detects the presence of Websense components and offers you options for modifying your installation. For information about adding or removing Websense components, see [Adding Components](#), page 163 and [Removing Components](#), page 173.

A **Typical** installation gives you the opportunity to install the following Websense components together on the same Solaris or Linux machine:

- ◆ Filtering Service

- ◆ Policy Server
- ◆ User Service
- ◆ Websense Manager
- ◆ Network Agent
- ◆ eDirectory Agent
- ◆ Logon Agent
- ◆ RADIUS Agent
- ◆ Usage Monitor

If some components need to be installed on separate machines, see *Installing Websense Components Separately*, page 101 for instructions to install individual Websense components.

To install Websense Enterprise/Web Security Suite on a Solaris or Linux machine:

1. Log on to the installation machine as the **root** user.
2. Close all applications and stop any antivirus software.
3. Create a setup directory for the installer files.  
For example: `/root/Websense_setup`
4. Obtain an installer package for Websense Enterprise/Web Security Suite:

**Web download:** To download an installer package, go to [www.websense.com](http://www.websense.com), and then navigate to the Downloads page.

- Choose your product, the dynamic (online) or full (offline) installer package, the operating system, and the language.

---

 **Note**

The **Dynamic** installer is an **online** installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.

The **Full** installer is a complete **offline** installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install the Websense Enterprise/Web Security Suite components. Use this package if you experience difficulties with the online installer.

---

- Save the selected installer package to the setup directory on the installation machine.
5. In the setup directory, enter the following command to unzip the file:  
`gunzip <download file name>`  
 For example: `gunzip Websense63Setup_Slr.tar.gz`
  6. Expand the file into its components with the following command:  
`tar xvf <unzipped file name>`  
 For example: `tar xvf Websense63Setup_Slr.tar`  
 This places the following files into the setup directory:

File	Description
install.sh	Installation program.
Setup	Archive file containing related installation files and documents.
Documentation	Release Notes: An HTML file containing release notes and last minute information about the Websense software. Read this file with any supported browser.

7. Run the installation program from the setup directory with the following command:  
`./install.sh`  
 To run the GUI version of the installer, use the following command:  
`./install.sh -g`  
 If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.
8. Follow the onscreen instructions through the subscription agreement.
9. Provide the installer with the following information.
  - **Product selection** (*Web Security Suite only*): Select the Web Security Suite edition you want to install:
    - **Web Security Suite:** Provides web security and reporting features.
    - **Web Security Suite and Client Policy Manager:** Provides web security and reporting features, plus desktop security.

The installer displays information about the required installation sequence for the components of this product on your operating system. Installing in the proper sequence is important because of the shared components.

- **Installation type:** You are asked to select an installation type:
  - **Typical:** Installs Filtering Service, Policy Server, Websense Manager, User Service, Usage Monitor, and Network Agent together on the same machine. The installer gives you the option of installing the following transparent identification agents: eDirectory Agent, Logon Agent, and RADIUS Agent.
  - **Custom:** Allows you to install individual Websense components. You can use this option to install components on separate machines in your network. For more information, see [Installing Websense Components Separately, page 101](#)

Select **Typical** to install the listed Websense components.

- **Multiple IP addresses:** If the installation machine is multihomed, all enabled network interface cards (NICs) appear in a list. Select the IP address of the card to use for Websense communications.



### Important

Make sure you select a NIC in *normal* mode (cards with an IP address). Interface cards configured for *stealth* mode will appear in this list as well. If you select a stealth mode NIC for Websense communications, Websense services will not work.

---

- **Integration option:** Select **Integrated**.
- **Integration product:** Select **Check Point FireWall-1**.

- **Port numbers:** The installer automatically assigns default port numbers to the Policy Server (55806) and the Filtering Service (15868). If either of these default ports is in use, the installer asks you to enter an alternate port. Enter an unused port number between 1024 and 65535.



**Note**

Record the port numbers if you change them from the defaults. You will need them when installing other Websense components.

---

- **Subscription key:** You can download the Websense Master Database during installation if you provide a valid subscription key or evaluation key. This will enable the Websense software to begin filtering immediately.
  - **I have a Websense subscription key:** If you have a valid subscription key, select this option and enter your key when prompted. You will be given the option to download the Websense Master Database during installation.
  - **I do not wish to use a key at this time:** Select this option to continue the installation without entering a key. You will not be given the option to download the Websense Master Database during installation. You can download the Master Database after installation by entering your key in Websense Manager. For instructions, see *Subscription Key and Master Database Download*, page 190.

To request a 30-day evaluation key, go to:

<http://www.websense.com/evaluations/>

- **Firewall installation warning:** The installer warns you that Network Agent cannot function properly on a machine that is being used as a firewall. (The exception is a blade server that has separate processors to accommodate Websense software and the Firewall-1 software.)

Select **Yes** or **No** to continue:

- If the installation machine is *not* being used as a firewall, select **Yes** to install Network Agent.

- If you are installing on a firewall machine—for example, the FireWall-1 machine—select **No**. Installation of the rest of the Websense components will continue, but Network Agent will not be installed. Install Network Agent later on a machine that is not running a firewall.
- **Network Interface Card (NIC) selection:** If you are installing Network Agent, all enabled network interface cards (NICs) appear in a list. If the machine has multiple NICs, select the one to use for Network Agent. Be sure that this card has visibility into the internet traffic you want Network Agent to filter.



**Note**

After installation, you can run the Traffic Visibility Tool to test whether the selected NIC can see the appropriate user internet traffic. See *Testing Visibility of Internet Traffic to Network Agent*, page 204.

---

- **Network Agent Feedback:** If you are installing Network Agent, the installer asks if you want to allow Websense, Inc., to gather information about the use of Websense-defined protocols.



**Note**

Network Agent never sends Websense, Inc., any information that would identify specific users, no matter which Network Agent feedback option is selected.

---

- **Initial filtering options:** Websense software can be configured to filter internet traffic immediately after installation, based on a predefined default policy, or to monitor internet traffic only. Select **Yes** to filter traffic initially, or **No** if you prefer to evaluate your network traffic before applying any type of filtering. You can install one or more of the Websense Reporting Tools to report on network activity.
- **Transparent user identification:** Select one of the following:
  - **eDirectory Agent:** Select this option to install eDirectory Agent to authenticate users transparently with Novell eDirectory Service.



- **Logon Agent:** Select this option to install Logon Agent to authenticate users transparently when they log on to the domain. Logon Agent receives its user information from an application called `LogonApp.exe` that must be run by a logon script in your network. For instructions, see [Creating and Running the Script for Logon Agent](#), page 196.
- **None:** This option does not install a Websense transparent identification agent. Select this option if you plan to configure authentication of users through Check Point FireWall-1.



**Note**

You can configure manual authentication in Websense Manager after installation. For instructions, see the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

---

- **RADIUS Agent:** If you have remote users who are authenticated by a RADIUS server, you can choose to install RADIUS Agent to transparently identify them.
- **Directory Access for DC Agent:** If you selected DC Agent for installation, you must provide a user name and a password with administrative privileges on the domain. DC Agent needs access to directory information to be able to identify users transparently.



**Note**

If you cannot install DC Agent with the appropriate privileges on the domain, you can configure them after installation. For instructions, see [Configure Domain Administrator Privileges](#), page 207.

---

- **Samba Client:** The installer warns that you must install the Samba client (v2.2.8a and later) to display protocol block messages and onscreen alerts on Windows workstations. You may continue Websense installation and download the Samba client later.



### Note

The Samba client controls the display of protocol block messages and onscreen alerts only:

- ◆ The Samba client must be installed on Linux and Solaris User Service machines in order to display protocol block messages on Windows workstations. However, it is *not* required for protocol blocking to occur.
- ◆ The Samba client must be installed on Linux and Solaris Policy Server machines in order to display onscreen alerts on Windows workstations.

---

To download the Samba client:

- *Solaris:* Go to the Sun freeware website at: [www.sunfreeware.com](http://www.sunfreeware.com)
- *Linux:* Go to: <http://rpmfind.net/linux/RPM>
- **Web browser:** You must provide the full path to the web browser you want to use when viewing online Help. This information is requested for installing Websense Manager.
- **Installation directory:** Enter the path to the directory where you want to install the Websense components, or accept the default location (`/opt/Websense`). If this directory does not already exist, the installer will create it.



### Important

The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

- 
- **System requirements check:** The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

If a disk space or memory error is displayed, check the *Deployment Guide* for system recommendations.

- **Installation summary:** A summary list appears, showing the installation path, the installation size, and the components that will be installed.

10. Select **Next** to begin the installation.

The Download Manager copies the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.

The installer creates the `/opt/Websense` directory, and the `/opt/Websense/Manager` directory if you installed Websense Manager. It also sets up the necessary files, including `/etc/rc3.d/S11WebsenseAdmin`, which enables Filtering Service to start automatically each time the system starts.

- If you did not install Network Agent, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Select **Next** to continue.
- **Master Database Download:** If you provided a valid subscription key when prompted, you are asked if you want to download the Websense Master Database now or at a later time using Websense Manager. Select a database download option and select **Next** to continue.



**Note**

The Master Database can take a few minutes or more than 60 minutes to download, decompress, and load into local memory.

---

If you selected to download the Master Database now, the download begins. The database must first be downloaded from the internet, and then decompressed and loaded into local memory. Downloading the

database from the internet can take a few minutes or more than 30 minutes, depending on factors such as internet connectivity, bandwidth, time of day, and your location relative to the download server. Decompressing and loading the database can take a few minutes or more than 30 minutes, depending on factors such as available memory, free disk space, and server process utilization.

When the database has finished loading, a message appears advising you of the status of the download. Select **Next** to continue.

11. When a message announcing successful completion of the installation is displayed:
  - If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions to update Websense components with text in the selected language.
  - If you chose an English language installer:
    - If you are installing in command line mode, select **Finish** to exit the installer.
    - If you are installing in GUI mode, select **Next** to continue. The installer asks if you want to start Websense Manager. Make a choice and select **Finish** to exit the installer.

See the *Administrator's Guide* for instructions on using Websense Manager.
12. If you stopped your antivirus software, be sure to start it again.
13. See [Chapter 5: Initial Setup](#) to perform post-installation tasks.
14. See [Chapter 6: Using FireWall-1 with Websense Software](#) to learn how Websense software works with FireWall-1, then follow the instructions in [Chapter 7: Configuring FireWall-1 NG, NG with AI, and NGX](#) to define the necessary objects and rules to support Websense filtering.



#### Note

If you decide to change the location of a Websense component, add functionality, or repair a component, run the Websense installer again on the machine you want to modify and select the appropriate option. The installer detects the presence of Websense components and offers you options for modifying your installation. For instructions, see [Modifying an Installation](#), page 163.

---

If you are installing Websense to also filter Citrix users, see Chapter 5 of the Websense Installation Guide for Integrated Citrix Servers for instructions to install the Citrix Integration Service and configure your integration.

## Installing Websense Components Separately

---

All Websense Enterprise/Web Security Suite components can be installed separately using the **Custom** installation path in the Websense installer. Use a Custom installation if your environment requires you to distribute Websense components on different machines in your network. The Remote Filtering components can be installed only through a Custom installation.

This section describes the procedures for installing the following Websense components separately. It is assumed that Policy Server and Filtering Service are on a different machine.



### Important

When installing Websense components separately, Policy Server must be installed first. Only Websense Manager can be installed before Policy Server.

---

- ◆ **Websense Manager:** Websense Manager installs on Windows, Solaris, and Linux. It can connect to a Policy Server on the same operating system or on a different operating system.
- ◆ **Network Agent:** Network Agent can be installed on Windows, Solaris, and Linux machines and must be able to see all internet traffic, both inbound and outbound.
- ◆ **DC Agent:** DC Agent runs on Windows and is installed in networks that use a Windows directory service (NTLM-based or Active Directory). To retrieve user information from the domain controller, DC Agent must be installed with domain administrator privileges on the network.
- ◆ **Real-Time Analyzer (RTA):** RTA installs on Windows only. You can have only one instance of RTA for each Policy Server in your network.
- ◆ **RADIUS Agent:** RADIUS Agent installs on Windows, Solaris, and Linux. RADIUS Agent can be used in conjunction with either Windows- or LDAP-based directory services; it works together with a RADIUS

client and RADIUS server to transparently identify users logging on from remote locations.

- ◆ **eDirectory Agent:** eDirectory Agent installs on Windows, Solaris, and Linux, and is installed in networks that use Novell eDirectory to identify users.
- ◆ **Logon Agent:** Logon Agent installs on Windows, Solaris, and Linux. Logon Agent receives user information at logon from a client application called `LogonApp.exe`, which must be run by a logon script. Instructions for creating and running this logon script in your network can be found in [Creating and Running the Script for Logon Agent](#), page 196. `LogonApp.exe` runs only on Windows client machines.



#### Note

The installation of these Websense components in the presence of other Websense components requires fewer steps. The installer searches for existing Websense initialization files and automatically uses this configuration information to locate the Policy Server and Filtering Service in the network.

---

- ◆ **Remote Filtering components:** The Remote Filtering components—Remote Filtering Server and Remote Filtering Client Pack—are required only if you need to enable web filtering on user workstations located outside your organization’s network firewall. These optional components are only available through a **Custom** installation.



#### Note

To enable the Remote Filtering components, you must subscribe to the remote filtering service.

---

- **Remote Filtering Server:** The Remote Filtering Server installs on Windows, Solaris, and Linux. It must be able to communicate with the Websense Filtering Service and with the Remote Filtering Clients installed on user workstations.
- **Remote Filtering Client Pack:** The Remote Filtering Client Pack is an installer used to deploy the **Remote Filtering Client** to Windows workstations that will be used outside the network firewall. The Remote Filtering Client Pack installs on Windows only.

Be sure to read the *Deployment Guide* for Websense Enterprise/Web Security Suite before beginning installation to determine the best way to distribute Websense Enterprise/Web Security Suite components in your network.

## Windows Procedures

The steps in this section are common to all installations of Websense Enterprise/Web Security Suite components on Windows. Start here to download and run the Websense installer, and then refer to the appropriate sections for the component-specific procedures.

To install components separately on Windows:

1. Log on to the installation machine with **local** administrator privileges.



### Important

If you are installing User Service or DC Agent, log on with **domain** as well as **local** administrator privileges. User Service and DC Agent must have administrator privileges on the network to retrieve user login information from the domain controller. Without this information, Websense software cannot filter by users and groups. If you cannot install these components with such privileges, you can configure administrator privileges for these services after installation. For instructions, see *Configure Domain Administrator Privileges*, page 207.

---

2. Close all applications and stop any antivirus software.
3. Obtain an installer package for Websense Enterprise/Web Security Suite:  
**Web download:** To download an installer package, go to [www.websense.com](http://www.websense.com), and then navigate to the Downloads page.
  - a. Choose the dynamic (online) or full (offline) installer package, the operating system, and the language.



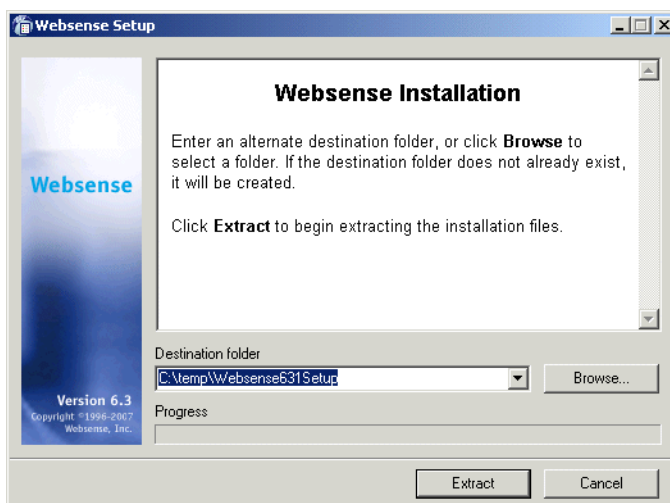
**Note**

The **Dynamic** installer is an **online** installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.

The **Full** installer is a complete **offline** installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install the Websense Enterprise/Web Security Suite components. Use this package if you experience difficulties with the online installer.

- b. Download the selected installer package to a folder on the installation machine, and double-click to extract the installer files.

A screen displays instructions for extracting the setup program.



Websense Installer File Extraction

- 4. If you do not want to accept the default location, click **Browse** to select a destination folder, or type in a path.



If the path you enter does not exist, the installer will create it for you.



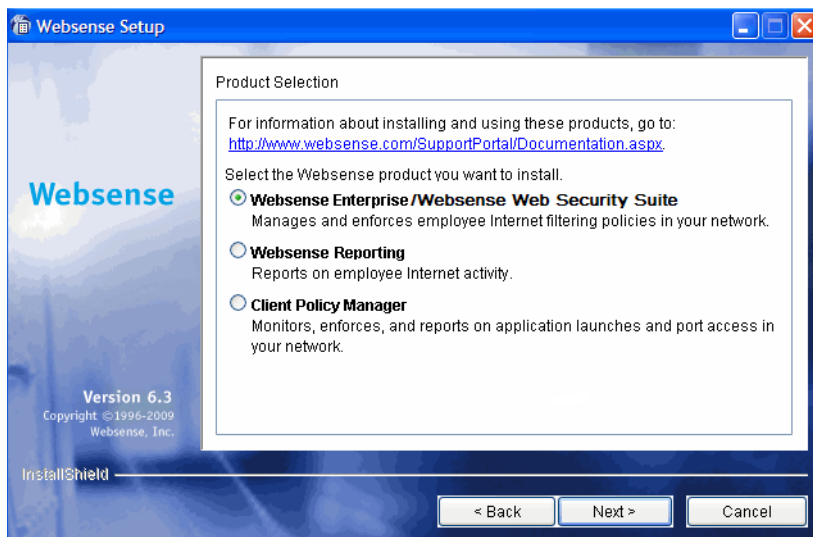
### Important

Do not extract the installer files to a folder on your desktop. This may prevent the Real-Time Analyzer from receiving the IP address of the Policy Server machine. Accept the default location of `C:\temp` or select another appropriate folder.

---

5. Click **Extract** to begin decompressing the files.
  - If Websense installation files already exist in that location, you may choose to overwrite the existing files.
  - A progress bar shows the status of the extraction, and the view pane scrolls a list of the files as they are decompressed.
  - `Setup.exe` runs automatically after the files are decompressed.
6. Click **Next** in the welcome screen and follow the onscreen instructions through the subscription agreement.

7. In the Product Selection screen, select the product to install and click **Next**:
  - *Websense Enterprise/Web Security Suite installer*: Select **Websense Enterprise/Websense Web Security Suite**.



Websense Product Selection

8. Select **Custom** and click **Next**.
9. To continue, proceed to the appropriate component section below.

## Websense Manager

Websense Manager, the administrative interface for your Websense software, can be installed in multiple locations in your network for convenient access. The Websense Manager machine needs network access to the Policy Server machine.

To install Websense Manager on a Windows machine:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 103.
2. Following the **Custom** installation path brings you to the component selection screen. Select **Websense Manager** and click **Next**.

A dialog box appears, asking you to select an installation directory for Websense Manager.

3. Accept the default path (C:\Program Files\Websense) or click **Browse** to locate another installation folder, and then click **Next** to continue.

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary list appears, showing the installation path, the installation size, and the components that will be installed.

4. Click **Next** to start the installation.

The Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

A message announcing the successful completion of the installation is displayed.

5. Click **Next** to continue.
  - If you chose a non-English language installer, the Websense Language Pack installer starts. Click **Next** in the welcome screen and follow the onscreen instructions.
  - If you chose an English language installer, a screen appears asking if you want to launch Websense Manager. If you do not want to launch Manager, clear the checkbox. Click **Finish** to exit the installer.
6. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

## Network Agent

Network Agent must be able to monitor 2-way internet traffic from the internal network. Install Network Agent on a machine that can see the internet requests *from* the internal network as well as the internet response *to* the requesting workstations.



### Important

If you install Network Agent on a machine that cannot monitor the targeted traffic, Network Agent features such as Protocol Management, Bandwidth Optimizer, and IM Attachment Manager will not perform as expected.

---

If this installation is part of a multiple deployment of the Network Agent (for load balancing purposes), you must be sure that the IP address ranges for each instance of the Network Agent do not overlap. Overlapping ranges result in double logging. Deploy the Network Agents so that they can filter the entire network.

Partial deployment results in incomplete filtering by protocol and bandwidth, as well as the loss of log data from network segments not watched by Network Agent.

To define IP address ranges for multiple Network Agents, follow the instructions in the *Administrator's Guide* for Websense Enterprise/Web Security Suite. For detailed information about deploying Network Agent, see the *Deployment Guide* for Websense Enterprise/Web Security Suite.

Do not install Network Agent on a machine running any type of firewall. Network Agent uses a packet capturing utility which may not work properly when installed on a firewall machine.

If you are attempting to install Network Agent on a machine on which the Filtering Service and Policy Server are already installed, see the procedures in [Adding Components](#), page 163.



### Important

The Websense Filtering Service and the Policy Server must be installed and running prior to installing Network Agent, or installed at the same time as Network Agent. The installer asks for the IP addresses and port numbers of these components and will not install Network Agent if the Policy Server and Filtering Service cannot be located.

---

To install Network Agent on a Windows machine:

1. Download and start the Windows installer using the procedure in [Windows Procedures](#), page 103.
2. Following the **Custom** installation path brings you to the component selection screen. Select **Network Agent** and click **Next**.

The installer asks you to identify the machine on which the Policy Server is installed.



### Note

The configuration port (55806) in this dialog box is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number in this dialog box.

---

3. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then click **Next**.

The installer asks you if this machine is running a firewall. Make sure that the installation machine is not being used as a firewall before continuing.



### Important

Network Agent cannot function properly on a machine running a firewall.

The only exception is a blade server or appliance that has separate processors or virtual processors to accommodate Network Agent and the firewall software.

---

4. Select **Yes** or **No** and click **Next** to continue:
  - Select **Yes** if the installation machine is *not* being used as a firewall. Installation will continue.
  - Select **No** if you are attempting to install Network Agent on a firewall machine, and Setup will exit. Install Network Agent on a machine that is not running a firewall.

A screen appears asking you to select the network interface card (NIC) that you want Network Agent to use for capturing traffic. All network interface cards enabled in the machine appear in a list.

5. If the machine has multiple NICs, select the one that has visibility into the internet traffic you want Network Agent to filter.



### Note

After installation, you can run the Traffic Visibility Tool to test whether the selected NIC can see the appropriate user internet traffic. See [Testing Visibility of Internet Traffic to Network Agent](#), page 204.

---

6. Click **Next** to continue.

The installer asks you to identify the machine on which the Websense Filtering Service is installed.



### Note

The communication port (15868) in this dialog box is the default port number used by the installer to install Filtering Service. If you installed Filtering Service using a different port number, enter that port number in this dialog box.

---

7. Enter the IP address of the Filtering Service machine, and the port number if different from the default, and then click **Next**.

A screen appears asking if you want to allow Websense, Inc., to gather information about the use of Websense-defined protocols. Information will be used in the development of protocol filtering.



**Note**

Network Agent never sends Websense, Inc., any information that would identify specific users, no matter which Network Agent feedback option is selected.

---

8. Select a Network Agent feedback option and click **Next** to continue.

The installer asks you to select an installation folder for the Websense components.

9. Accept the default path (C:\Program Files\Websense) or click **Browse** to locate another installation folder, and then click **Next** to continue.

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary list appears, showing the installation path, the installation size, and the components that will be installed.

10. Click **Next** to start the installation.

The Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

11. When a message announcing successful completion of the installation is displayed:

- If you chose a non-English language installer, click **Next** to continue.

The Websense Language Pack installer starts. Click **Next** in the welcome screen and follow the onscreen instructions.

- If you chose an English language installer, click **Finish** to exit the installer.
12. If you stopped your antivirus software, remember to start it again after Websense components have been installed.
  13. Configure Network Agent for use in your network. See the instructions for initial configuration of Network Agent in [Chapter 5: Initial Setup](#), as well as the Network Agent chapter in the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

## DC Agent

DC Agent is a Websense transparent identification agent used in networks that authenticate users with a Windows directory service (NTLM-based or Active Directory). You can choose to install DC Agent during a Typical Websense installation on Windows or Linux. If you did not install it, and you need to authenticate through a Windows-based directory service, you can install DC Agent on a Windows machine with the following procedure.

If your network is large, you may benefit from installing DC Agent on multiple machines. This way, you will have ample space for DC Agent files that are continually populated with user information. For additional information about how to deploy DC Agent, see [Websense Enterprise/Web Security Suite Components](#), page 15.

Do not install DC Agent on the same machine as eDirectory Agent, as this can cause conflicts.

To install DC Agent on a Windows machine:

1. Download and start the Windows installer using the procedure in [Windows Procedures](#), page 103.
2. Following the **Custom** installation path brings you to the component selection screen. Select **DC Agent** and click **Next**.

If the installation machine is multihomed, all enabled network interface cards appear in a list.

3. Select the IP address of the card you want DC Agent to use to communicate and click **Next**.



The installer asks you to identify the machine on which the Policy Server is installed.



**Note**

The configuration port (55806) in this dialog box is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number in this dialog box.

---

4. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then click **Next**.

The installer asks you to provide a user name and a password with administrative privileges on the domain. DC Agent needs access to directory information to be able to identify users transparently.

5. Enter the domain and user name, followed by the network password for an account with domain administrator privileges, and then click **Next**.



**Note**

You can also grant domain administrator privileges to DC Agent after installation. For instructions, see [Configure Domain Administrator Privileges](#), page 207.

---

The installer asks you to select an installation folder for the Websense components.

6. Accept the default path (C:\Program Files\Websense) or click **Browse** to locate another installation folder, and then click **Next** to continue.

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.

- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary list appears, showing the installation path, the installation size, and the components that will be installed.

7. Click **Next** to start the installation.

The Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

8. When a message announcing successful completion of the installation is displayed:
  - If you chose a non-English language installer, click **Next** to continue. The Websense Language Pack installer starts. Click **Next** in the welcome screen and follow the onscreen instructions.
  - If you chose an English language installer, click **Finish** to exit the installer.
9. If you stopped your antivirus software, remember to start it again after Websense components have been installed.
10. Configure User Service to communicate with DC Agent by following the instructions in the User Identification chapter of the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

## Real-Time Analyzer (RTA)

RTA graphically displays bandwidth usage information and shows requests by category or protocol. RTA installs on Windows only. You can have only one instance of RTA for each Policy Server in your network.

To install RTA on a Windows machine:

1. Download and start the Windows installer using the procedure in [Windows Procedures, page 103](#).
2. Following the **Custom** installation path brings you to the component selection screen. Select **Real-Time Analyzer** and click **Next**.

If the installation machine is multihomed, all enabled network interface cards appear in a list.

3. Select the IP address of the card you want RTA to use to communicate and click **Next**.

The installer asks you to identify the machine on which the Policy Server is installed.



**Note**

The configuration port (55806) in this dialog box is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number in this dialog box.

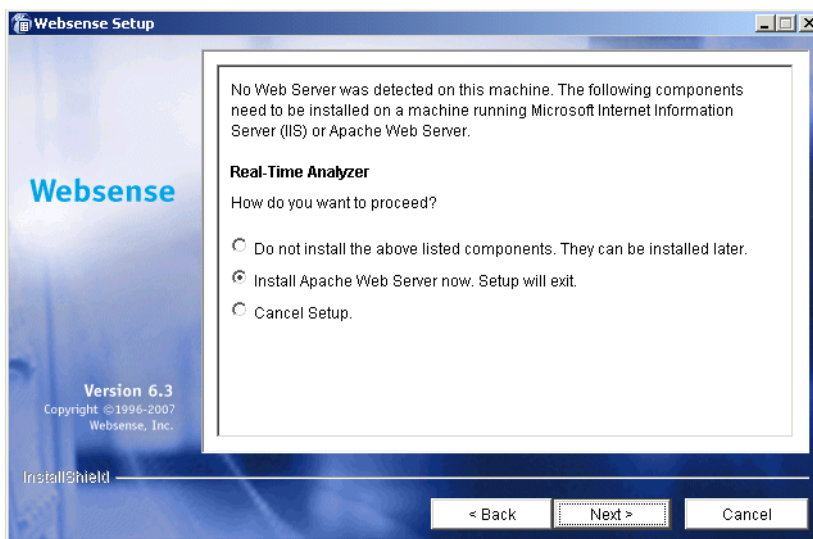
---

4. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then click **Next**.

The installer checks your system for a supported web server (Apache HTTP Server or IIS) for the Real-Time Analyzer and takes the following action:

- If both supported web servers are detected, a dialog box appears asking you to choose one server for RTA.
- If one of the supported servers is detected, the installer continues. No notification appears.

- If neither supported web server is detected, the installer gives you the option to install the Apache HTTP Server or continue the installation without installing RTA.



#### Web Server for Real-Time Analyzer

If you select the Apache HTTP Server installation option, the Websense installer starts the Apache installer and exits without installing any Websense components. You must restart your computer after installing the Apache HTTP Server and run the Websense installer again.

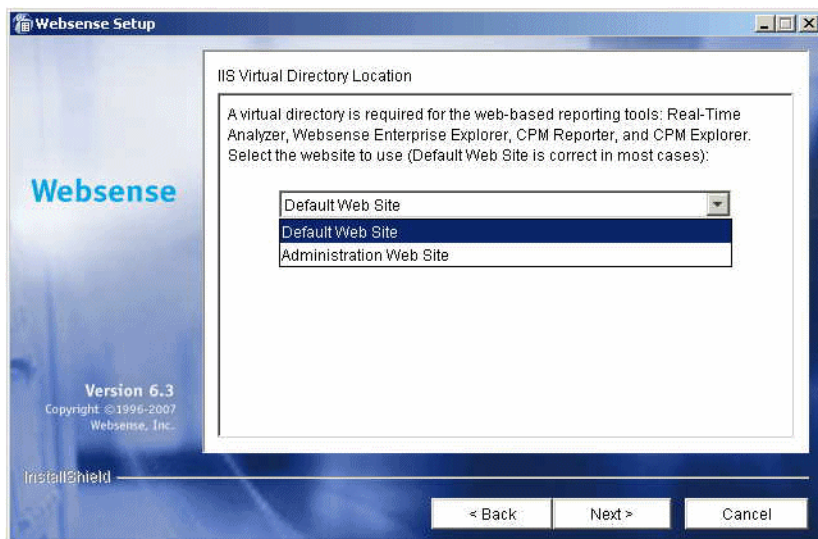


#### Note

Apache HTTP Server documentation is installed in HTML format in the `docs/manual/` directory. It is also available at: <http://httpd.apache.org/docs/2.0/>.

---

5. Select a web server installation option and click **Next** to continue.  
If you are using IIS as your web server, you are prompted to select the name of the website in the IIS Manager under which the installer should create a virtual directory. The default value is **Default Web Site**, which is correct in most instances.



Virtual Directory Selection

6. If you have renamed the default website in the IIS Manager or are using a language version of Windows other than English, select the proper website from the names in the drop-down list, and then click **Next** to continue.

The installer asks you to select an installation folder for the Websense components.

7. Accept the default path (C:\Program Files\Websense) or click **Browse** to locate another installation folder, and then click **Next** to continue.

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary list appears, showing the installation path, the installation size, and the components that will be installed.

8. Click **Next** to start the installation.

The Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

9. When a message announcing successful completion of the installation is displayed:
  - If you chose a non-English language installer, click **Next** to continue. The Websense Language Pack installer starts. Click **Next** in the welcome screen and follow the onscreen instructions.
  - If you chose an English language installer, click **Finish** to exit the installer.



#### Note

Before you can access Real-Time Analyzer and other Websense Reporting Tools, you must first log on to Websense Manager and configure user permissions. For more information, see the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

---

10. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

## RADIUS Agent

The Websense RADIUS Agent allows you to integrate your Websense filtering policies with authentication provided by a RADIUS server. RADIUS Agent enables Websense software to transparently identify users who access your network using a dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), or other remote connection.

To install the RADIUS Agent on a Windows machine:

1. Download and start the Windows installer using the procedure in [Windows Procedures, page 103](#).

2. Following the **Custom** installation path brings you to the component selection screen. Select **RADIUS Agent** and click **Next**.

The installer asks you to identify the machine on which the Policy Server is installed.



**Note**

The configuration port (55806) in this dialog box is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number in this dialog box.

---

3. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then click **Next**.

If the installation machine is multihomed, all enabled network interface cards (NICs) with an IP address appear in a list.

4. Select the IP address of the card you want RADIUS Agent to use to communicate and click **Next**.

The installer asks you to select an installation folder for the Websense components.

5. Accept the default path (C:\Program Files\Websense) or click **Browse** to locate another installation folder, and then click **Next** to continue.

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary list appears, showing the installation path, the installation size, and the components that will be installed.

6. Click **Next** to start the installation.

The Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

7. When a message announcing successful completion of the installation is displayed:
  - If you chose a non-English language installer, click **Next** to continue. The Websense Language Pack installer starts. Click **Next** in the welcome screen and follow the onscreen instructions.
  - If you chose an English language installer, click **Finish** to exit the installer.
8. If you stopped your antivirus software, remember to start it again after Websense components have been installed.
9. Configure the RADIUS Agent, and configure your environment for RADIUS Agent. For instructions, see the User Identification chapter in the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

## eDirectory Agent

The Websense eDirectory Agent works together with Novell eDirectory to identify users transparently so that Websense software can filter them according to particular policies assigned to users or groups.

Do not install eDirectory Agent on the same machine as DC Agent or Logon Agent, as this can cause conflicts.

To install the eDirectory Agent on a Windows machine:

1. Download and start the Windows installer using the procedure in [Windows Procedures, page 103](#).
2. Following the **Custom** installation path brings you to the component selection screen. Select **eDirectory Agent** and click **Next**.



The installer asks you to identify the machine on which the Policy Server is installed.



**Note**

The configuration port (55806) in this dialog box is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number in this dialog box.

3. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then click **Next**.

If the installation machine is multihomed, all enabled network interface cards (NICs) with an IP address appear in a list.

4. Select the IP address of the card you want eDirectory Agent to use to communicate and click **Next**.

The installer asks for the Novell eDirectory name and password.

5. Enter the full *distinguished name* and a valid password, and then click **Next** to continue.

The installer asks you to select an installation folder for the Websense components.

6. Accept the default path (C:\Program Files\Websense) or click **Browse** to locate another installation folder, and then click **Next** to continue.

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary list appears, showing the installation path, the installation size, and the components that will be installed.

7. Click **Next** to start the installation.

The Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

8. When a message announcing successful completion of the installation is displayed:
  - If you chose a non-English language installer, click **Next** to continue. The Websense Language Pack installer starts. Click **Next** in the welcome screen and follow the onscreen instructions.
  - If you chose an English language installer, click **Finish** to exit the installer.
9. If you stopped your antivirus software, remember to start it again after Websense components have been installed.
10. Configure the eDirectory Agent and Novell eDirectory by following the instructions in the User Identification chapter of the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

## Logon Agent

Logon Agent is a Websense transparent identification agent that detects users as they log on to Windows domains in your network via client machines. The Logon Agent receives logon information from `LogonApp.exe`, a separate client application that runs only on Windows client machines, and must be run by a logon script. For information about setting up this script in your network, see [Creating and Running the Script for Logon Agent](#), page 196.

Logon Agent can be run together with DC Agent if some of the users in your network are not being authenticated properly. This might happen if your network uses Windows 98 workstations, which do not permit DC Agent to poll users for their identification when they make an internet request.

Do not install Logon Agent on the same machine as eDirectory Agent, as this can cause conflicts.

To install the Logon Agent on a Windows machine:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 103.
2. Following the **Custom** installation path brings you to the component selection screen. Select **Logon Agent** and click **Next**.

The installer asks you to identify the machine on which the Policy Server is installed.



**Note**

The configuration port (55806) in this dialog box is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number in this dialog box.

---

3. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then click **Next**.

If the installation machine is multihomed, all enabled network interface cards (NICs) with an IP address appear in a list.

4. Select the IP address of the card you want Logon Agent to use to communicate and click **Next**.

The installer asks you to select an installation folder for the Websense components.

5. Accept the default path (C:\Program Files\Websense) or click **Browse** to locate another installation folder, and then click **Next** to continue.

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary list appears, showing the installation path, the installation size, and the components that will be installed.

6. Click **Next** to start the installation.

The Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

7. When a message announcing successful completion of the installation is displayed:
  - If you chose a non-English language installer, click **Next** to continue. The Websense Language Pack installer starts. Click **Next** in the welcome screen and follow the onscreen instructions.
  - If you chose an English language installer, click **Finish** to exit the installer.
8. If you stopped your antivirus software, remember to start it again after Websense components have been installed.
9. Set up the required logon script by following the instructions in [Creating and Running the Script for Logon Agent](#), page 196.
10. Configure Logon Agent to communicate with client workstations and the Filtering Service by following the instructions in the User Identification chapter of the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

## Remote Filtering Server

The Remote Filtering Server provides web filtering for user workstations located outside the network firewall. In order to be filtered through the Remote Filtering Server, a remote workstation must be running the Remote Filtering Client. (For Remote Filtering Client installation instructions, see [Remote Filtering Client](#), page 132.)



### Note

To enable the Remote Filtering components, you must subscribe to the remote filtering service.

---

The Remote Filtering Server should be installed on a separate, dedicated machine. This machine must be able to communicate with the Websense Filtering Service and with the remote workstations outside the network firewall. The Remote Filtering Server machine does not have to be joined to a domain.

The Remote Filtering Server should be installed inside your organization's outermost network firewall, but in the DMZ outside the firewall that protects the rest of the corporate network. For more information about deploying the Remote Filtering Server in your network, see the *Remote Filtering* section in the *Deployment Guide* for Websense Enterprise/Web Security Suite.

To provide failover capability for the primary Remote Filtering Server, you can install secondary and tertiary Remote Filtering Servers. Each Remote Filtering Client can be configured to connect with a primary, secondary, and tertiary Remote Filtering Server. If the primary server is unavailable, the client attempts to connect with the secondary, then the tertiary, then the primary again, and so on.



### Important

- ◆ Install only one primary Remote Filtering Server for each Filtering Service in your network.
  - ◆ Do not install the Remote Filtering Server on the same machine as the Filtering Service or Network Agent.
  - ◆ Remote Filtering Server is supported on Windows Server® 2003 only if Service Pack 1 has been installed.
  - ◆ Do not enable DHCP on the Remote Filtering Server machine.
- 

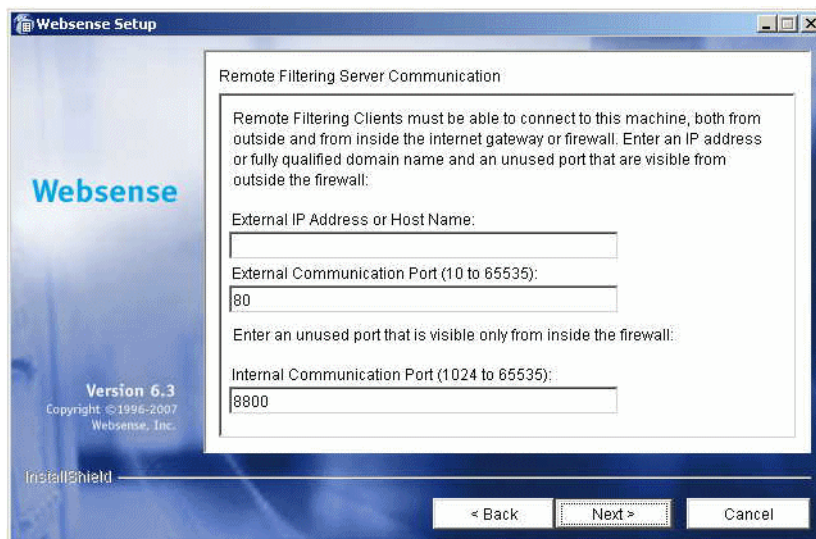
To install the Remote Filtering Server on a Windows machine:

1. Download and start the Windows installer using the procedure in [Windows Procedures, page 103](#).
2. Following the **Custom** installation path brings you to the component selection screen. Select **Remote Filtering Server** and click **Next**.

If the installation machine is multihomed, all enabled network interface cards appear in a list.

3. Select the IP address of the card you want the Remote Filtering Server to use to communicate with other Websense components inside the network firewall, and click **Next**.

Remote Filtering Clients must be able to connect to the Remote Filtering Server, both from inside and from outside the internet gateway or network firewall. The installer asks you to provide connection information for this machine.



Remote Filtering Server Communication

4. In the **External IP Address or Host Name** field, enter an IP address or machine name (in the form of a fully qualified domain name) that is visible from *outside* the network firewall.

5. In the **External Communication Port** field, enter a port number (from 10 to 65535) that is not in use, and that is accessible from *outside* the network firewall. The default value is 80. (If there is a web server installed on the machine, port 80 may already be in use, so you may need to change the default value.)



### Important

The port entered as the **External Communication Port** must be opened on your network firewall to accept connections from Remote Filtering Clients on workstations located outside the firewall. For more information, see [Firewall Configuration for Remote Filtering](#), page 209.

---

6. In the **Internal Communication Port** field, enter a port number (from 1024 to 65535) that is not in use, and that is accessible only from *inside* the network firewall. The default value is 8800.



### Important

Be sure that your network firewall is configured to block connections to the **Internal Communication Port** from workstations located outside the firewall. For more information, see [Firewall Configuration for Remote Filtering](#), page 209.

---

7. Click **Next** to continue.

The installer asks you to enter a pass phrase of any length for the Remote Filtering Server. This pass phrase will be combined with unpublished keys to create an encrypted authentication key (shared secret) for secure client/server communication.

8. Before selecting a **pass phrase**, consider the following requirements:
  - If Websense Client Policy Manager (CPM) is already installed in your network, you must enter the same pass phrase used when installing CPM.
  - If you install Websense Client Policy Manager (CPM) in your network in the future, you must use the pass phrase you enter in this screen.

- If you want this installation of the Remote Filtering Server to function as a backup (secondary or tertiary) server for a primary Remote Filtering Server, you must enter the same pass phrase used when installing the primary Remote Filtering Server.
- The pass phrase must include only ASCII characters. Do not use extended ASCII or double-byte characters.
- You must use the pass phrase you enter in this screen when you install the Remote Filtering Clients that will connect with this server. (See [Remote Filtering Server Connection Information](#), page 135.)



### Warning

Be sure to record your **pass phrase** and keep it in a safe place, as it cannot be retrieved from the Websense system later.

9. Enter and confirm your **pass phrase**.
10. Click **Next** to continue.

Remote Filtering Server must be able to communicate with the Websense Filtering Service. The installer asks you to identify the machine on which Filtering Service is installed.

Filtering Service Information



11. In the first field, enter the actual (internal) IP address of the Filtering Service machine.
12. Is there a firewall or other network device that performs network address translation between the Filtering Service machine and this machine?
  - If yes, enter the translated (external) IP address of the Filtering Service machine.
  - If no, click to deselect the checkbox and grey out the **Translated (external) IP address of Filtering Service** field.
13. Enter the filter port number for the Filtering Service machine, if it was changed from the default of 15868.



#### Note

The filter port is the default communication port used by the installer to install Filtering Service. If you installed Filtering Service using a different communication port, enter that port number.

---

14. Enter the block page port number for the Filtering Service machine, if it was changed from the default value of 15871.



#### Important

If there is a firewall between the Filtering Service machine and the Remote Filtering Server machine, be sure to open the filter port (15868) and block page port (15871) on that firewall. Filtering Service must be able to accept connections from the Remote Filtering Server, and serve block pages to remote users. For more information, see [Firewall Configuration for Remote Filtering, page 209](#).

---

15. Click **Next**.

The installer asks you to select an installation folder for the Websense components.

16. Accept the default path (C:\Program Files\Websense) or click **Browse** to locate another installation folder, and then click **Next** to continue.

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary list appears, showing the installation path, the installation size, and the components that will be installed.

17. Click **Next** to start the installation.

The Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

Since the Network Agent was not installed on this machine, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

18. When a message announcing successful completion of the installation is displayed:
  - If you chose a non-English language installer, click **Next** to continue. The Websense Language Pack installer starts. Click **Next** in the welcome screen and follow the onscreen instructions.
  - If you chose an English language installer, click **Finish** to exit the installer.
19. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

For more information about how remote filtering works, see the *Filtering Remote Clients* section in the *Administrator's Guide* for Websense Enterprise/ Web Security Suite.

## Remote Filtering Client Pack

The Remote Filtering Client Pack is an installer package that allows you to install the Remote Filtering Client. Once you have this installer package, you can use it to deploy the Remote Filtering Client on Windows workstations (see [Remote Filtering Client](#), page 132). The Remote Filtering Client Pack can be installed on Windows machines only.



### Note

To enable the Remote Filtering components, you must subscribe to the remote filtering service.

---

To install the Remote Filtering Client Pack on a Windows machine:

1. Download and start the Windows installer using the procedure in [Windows Procedures](#), page 103.
2. Following the **Custom** installation path brings you to the component selection screen. Select **Remote Filtering Client Pack** and click **Next**. The installer asks you to select an installation folder for the Remote Filtering Client Pack.
3. Accept the default path (C:\Program Files\Websense) or click **Browse** to locate another installation folder, and then click **Next** to continue.

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary list appears, showing the installation path, the installation size, and the components that will be installed.

4. Click **Next** to start the installation.

The Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

If Network Agent was not installed on this machine, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

5. When a message announcing successful completion of the installation is displayed:
  - If you chose a non-English language installer, click **Next** to continue. The Websense Language Pack installer starts. Click **Next** in the welcome screen and follow the onscreen instructions.
  - If you chose an English language installer, click **Finish** to exit the installer.
6. If you stopped your antivirus software, remember to start it again after Websense components have been installed.
7. If you accepted the default installation path in [Step 3](#), the Remote Filtering Client Pack can be found in the following location:  
C:\Program Files\Websense\bin\  
RemoteFilteringAgentPack\NO\_MSI\CPMClient.msi
8. Use the Remote Filtering Client Pack to install the Remote Filtering Client on user workstations that you want to filter when they are outside the network firewall. See [Remote Filtering Client](#), page 132 for details.

## Remote Filtering Client

The Remote Filtering Client is installed on workstations that will be used outside the network firewall. This component connects with a Remote Filtering Server located inside the network firewall to enable web filtering on the remote workstation. The Remote Filtering Client installs on Windows only.



### Note

To enable the Remote Filtering components, you must subscribe to the remote filtering service.

---

The Remote Filtering Client can be installed in the following ways:

- ◆ **Manual installation:** Use the Remote Filtering Client Pack to manually install the Remote Filtering Client on an individual workstation. See [Manual Installation of Remote Filtering Client](#), page 133 for information.
- ◆ **Automatic deployment with third-party tool:** Use the Remote Filtering Client Pack and a third-party deployment tool to automatically deploy the Remote Filtering Client to user workstations. See [Installing Remote Filtering Client with a Third-Party Deployment Tool](#), page 138 for information.
- ◆ **Deployment as part of CPM Client Agent (Websense Client Policy Manager™ users only):** If you purchased a subscription to the Websense Client Policy Manager™ (CPM), it is not necessary to install the Remote Filtering Client. The Remote Filtering Client application is included as part of the CPM Client Agent, and is deployed automatically when you deploy the CPM Client Agent to user workstations. See your Websense Client Policy Manager documentation for more information.



### Warning

Do not install the Remote Filtering Client on:

- ◆ Machines running Windows 2000, Service Pack 2 or earlier. The installation will fail. See the *Deployment Guide* for Websense Enterprise/Web Security Suite for information about system requirements.
  - ◆ Machines where you installed the Remote Filtering Server. A Remote Filtering Client running on the same machine as the Remote Filtering Server will eventually cause remote filtering to fail.
- 

## Manual Installation of Remote Filtering Client

To manually install the Remote Filtering Client on a single Windows workstation:

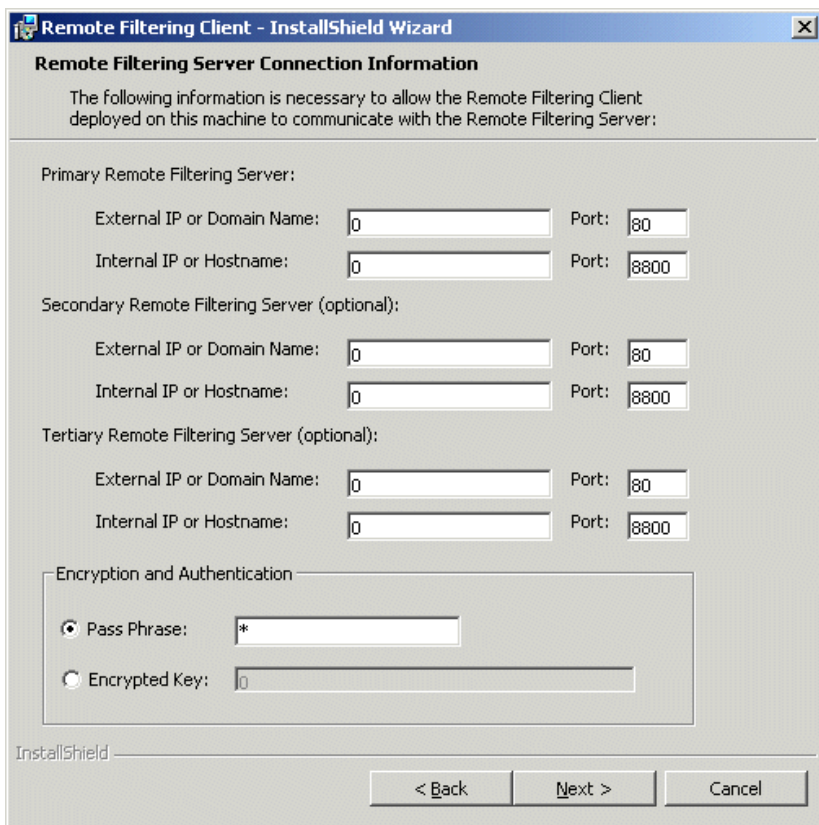
1. Make sure that the Remote Filtering Server with which this client will connect has been correctly installed on a separate machine. See [Remote Filtering Server](#), page 124 for Windows installation instructions; see [Remote Filtering Server](#), page 158 for Solaris and Linux installation instructions.

2. Install the Remote Filtering Client Pack on the workstation as described in *Remote Filtering Client Pack*, page 131. Or, if you have already installed the Remote Filtering Client Pack on another machine, you can simply copy the `CPMClient.msi` file to a folder on the installation workstation. If you selected the default installation path of `C:\Program Files\Websense`, this file will be located at:

```
C:\Program Files\Websense\bin\  
RemoteFilteringAgentPack\NO_MSI\CPMClient.msi
```

3. Double-click the `CPMClient.msi` file.  
The installer for Remote Filtering Client will open.
4. Click **Next** to continue.

Remote Filtering Clients must be able to connect with a Remote Filtering Server from outside your organization's internet gateway or firewall. You are asked to provide connection information for the Remote Filtering Servers that this client will use for web filtering.



The screenshot shows a dialog box titled "Remote Filtering Client - InstallShield Wizard". The main heading is "Remote Filtering Server Connection Information". Below this, a message states: "The following information is necessary to allow the Remote Filtering Client deployed on this machine to communicate with the Remote Filtering Server:". The form is divided into three sections for server configuration:

- Primary Remote Filtering Server:**
  - External IP or Domain Name: [0] Port: [80]
  - Internal IP or Hostname: [0] Port: [8800]
- Secondary Remote Filtering Server (optional):**
  - External IP or Domain Name: [0] Port: [80]
  - Internal IP or Hostname: [0] Port: [8800]
- Tertiary Remote Filtering Server (optional):**
  - External IP or Domain Name: [0] Port: [80]
  - Internal IP or Hostname: [0] Port: [8800]

At the bottom, there is an "Encryption and Authentication" section with two radio buttons:

- Pass Phrase: [\*]
- Encrypted Key: [0]

The bottom of the dialog features three buttons: "< Back", "Next >", and "Cancel". The "InstallShield" logo is visible in the bottom left corner.

Remote Filtering Server Connection Information

The Remote Filtering Client must be configured to connect with a primary Remote Filtering Server.

If optional secondary and tertiary Remote Filtering Servers were installed to provide failover capability for the primary server, the Remote Filtering Client must be configured to connect with these as well. The Remote Filtering Client will attempt to connect with the primary Remote Filtering Server first, then the secondary, then the tertiary, then the primary again, and so on.

5. In the **Primary Remote Filtering Server** section of the screen, enter connection information for the Remote Filtering Server that you want this client to attempt to connect with first:
  - Enter the externally visible IP address or fully qualified domain name (FQDN) of the primary Remote Filtering Server machine in the **External IP or Domain Name** field.



### Important

You must use the same external address in **the same address format**—IP address or FQDN—that you entered when you installed this Remote Filtering Server. That is, if you entered an IP address in the **External IP Address or Host Name** field when installing the Remote Filtering Server, you must enter the same IP address in this field. If you entered a machine name in the form of a fully qualified domain name (FQDN), you must enter the same FQDN here.

---

- In the **Port** field to the right of the **External IP or Domain Name** field, enter the port number for the externally visible port used to communicate with the primary Remote Filtering Server from outside the network firewall. This must be the same port entered in the **External Communication Port** field when this Remote Filtering Server was installed.
- Enter the internal IP address or the fully qualified domain name for the primary Remote Filtering Server machine in the **Internal IP or Hostname** field.
- In the **Port** field to the right of the **Internal IP or Hostname** field, enter the port number for the internal communication port on the primary Remote Filtering Server that can only be accessed from



inside the network firewall. This must be the same port entered in the **Internal Communication Port** field when this Remote Filtering Server was installed.



**Note**

If the Remote Filtering Client is on a notebook computer that is used both inside and outside the network firewall, this port allows the Websense software to determine where the machine is located and filter it appropriately. The machine will be filtered in the same way as an internal client when it is used inside the organization's network firewall, and by the Remote Filtering Service when it is used remotely.

6. If you have installed the optional secondary and tertiary Remote Filtering Servers to provide failover protection for the primary Remote Filtering Server, enter connection information for these servers in the **Secondary Remote Filtering Server** and **Tertiary Remote Filtering Server** sections of the screen.
7. In the **Encryption and Authentication** section, do one of the following:
  - Select **Pass Phrase** and enter the same pass phrase that was entered in the **Pass Phrase** field during installation of the primary Remote Filtering Server. (The secondary and tertiary Remote Filtering Servers must have the same pass phrase as their primary Remote Filtering Server.)

-OR-

  - Select **Encrypted Key** and enter the encrypted key (shared secret) created from the pass phrase and unpublished Remote Filtering Server keys. The encrypted key can be found in the `WSSEK.dat` file on the Remote Filtering Server machine. If you selected the default installation path, this file will be located at:
    - `C:\Program Files\Websense\bin\WSSEK.dat`  
on Windows machines, and
    - `/opt/Websense/bin/WSSEK.dat`  
on Solaris and Linux machines.
8. Click **Next** to continue.
9. Click **Install** to begin installation.

When the installer is finished, a message appears advising you that the procedure was successful.

10. Click **Finish** to exit the installer.
11. If a message appears indicating that you must restart the machine, click **Yes** to restart now. Remote filtering will not function properly until the machine is restarted.

If no message appears, restarting the machine is not required.

## **Installing Remote Filtering Client with a Third-Party Deployment Tool**

Before deploying the Remote Filtering Client to user workstations, make sure that the Remote Filtering Server with which these clients will connect has been correctly installed on a separate machine. See [Remote Filtering Server, page 124](#) for Windows installation instructions; see [Remote Filtering Server, page 158](#) for Solaris and Linux installation instructions.

To obtain the installer for the Remote Filtering Client, install the Remote Filtering Client Pack on a Windows machine (see [Remote Filtering Client Pack, page 131](#) for instructions). If you selected the default installation path of C:\Program Files\Websense, the installer is placed in the following location:

```
C:\Program Files\Websense\bin\  
RemoteFilteringAgentPack\NO_MSI\CPMClient.msi
```

To deploy the Remote Filtering Client to Windows workstations, use this installer with a third-party deployment tool, such as Microsoft® Systems Management Server (SMS) or Novell® ZENworks®.

### ***Command Line Parameters for Remote Filtering Client Installation***

This section provides the command line parameters required to install the Remote Filtering Client using a third-party deployment tool.

Remote Filtering Clients are installed on user workstations or notebook computers that are used outside your organization's internet gateway or firewall. These machines must be able to connect with a Remote Filtering Server that is located inside the internet gateway or firewall.

Each Remote Filtering Client must be configured to connect with a primary Remote Filtering Server. If optional secondary and tertiary Remote Filtering Servers were installed to provide failover capability for the primary server, the Remote Filtering Client must be configured to connect with these as well. The

Remote Filtering Client will attempt to connect with the primary Remote Filtering Server first, then the secondary, then the tertiary, then the primary again, and so on.

Below are the necessary command line parameters for installing the Remote Filtering Client with a third-party deployment tool:



### Note

These parameters are *not* case sensitive.

---

- ◆ The following parameters must be configured to allow the Remote Filtering Client to communicate with the **primary** Remote Filtering Server:
  - **PRIMARY\_WISP\_ADDRESS**=*<external IP address or FQDN of primary Remote Filtering Server>*

The externally visible address for the primary Remote Filtering Server machine, as entered in the **External IP Address or Host Name** field when the primary Remote Filtering Server was installed.



### Important

This must be the same external address in **the same address format**—IP address or FQDN—that was entered when this Remote Filtering Server was installed. That is, if you entered an IP address in the **External IP Address or Host Name** field when installing the Remote Filtering Server, you must enter the same IP address here. If you entered a machine name in the form of a fully qualified domain name (FQDN), you must enter the same FQDN here.

---

- **PRIMARY\_WISP\_PORT**=*<external port number of primary Remote Filtering Server>*

The port number for the externally visible port used to communicate with the primary Remote Filtering Server from outside the network firewall. This must be the same port entered in the **External Communication Port** field when this Remote Filtering Server was installed.

- **PRIMARY\_INTERNAL\_WISP\_ADDRESS**=<internal IP address or FQDN of primary Remote Filtering Server>

The internal address, visible from inside the network firewall, for the machine on which the primary Remote Filtering Server is installed.

- **PRIMARY\_INTERNAL\_WISP\_PORT**=<internal port number of primary Remote Filtering Server>

The port number for the internal communication port on the primary Remote Filtering Server that can only be accessed from inside the network firewall. This must be the same port entered in the **Internal Communication Port** field when the Remote Filtering Server was installed.

- ◆ If **secondary** and **tertiary** Remote Filtering Servers have been installed, use the following parameters to configure communication with them:

- **SECONDARY\_WISP\_ADDRESS**=<external IP address or FQDN of secondary Remote Filtering Server>

- **SECONDARY\_WISP\_PORT**=<external IP address or FQDN of secondary Remote Filtering Server>

- **SECONDARY\_INTERNAL\_WISP\_ADDRESS**=<internal IP address or FQDN of secondary Remote Filtering Server>

- **SECONDARY\_INTERNAL\_WISP\_PORT**=<internal IP address or FQDN of secondary Remote Filtering Server>

- **TERTIARY\_WISP\_ADDRESS**=<external IP address or FQDN of tertiary Remote Filtering Server>

- **TERTIARY\_WISP\_PORT**=<external IP address or FQDN of tertiary Remote Filtering Server>

- **TERTIARY\_INTERNAL\_WISP\_ADDRESS**=<internal IP address or FQDN of tertiary Remote Filtering Server>

- **TERTIARY\_INTERNAL\_WISP\_PORT**=<internal IP address or FQDN of tertiary Remote Filtering Server>

These addresses and port numbers must match those entered during installation of the Remote Filtering Servers, as noted above for the primary Remote Filtering Server.

- ◆ **PATH**=<installation path>

Directory where the Remote Filtering Client will be installed on each client workstation. If this parameter is not specified, the default

installation path is C:\PROGRAM FILES\Websense\WDC, and the WDC directory is hidden by default.

- ◆ **PASSPHRASE**=<pass phrase for Remote Filtering Server>

The **Pass Phrase** entered when the primary Remote Filtering Server was installed. Note that all Remote Filtering Servers in the same failover group (primary, secondary, and tertiary) must have the same pass phrase.

- ◆ **REBOOT=YES | NO | PROMPT | IF\_NEEDED\_PROMPT**

This parameter defines whether the client workstation is automatically restarted after the Remote Filtering Client is installed (or uninstalled). Values for this parameter are:

- **YES**: Machines are restarted, and employees are not prompted to restart.
- **NO**: Machines are not restarted, and employees are not prompted to restart.
- **PROMPT**: Employees are prompted to restart their machines.
- **IF\_NEEDED\_PROMPT**: Employees are prompted to restart their machines only if a restart is required. (Default.)



### Important

You must restart the workstation after installing the Remote Filtering Client if:

- ◆ The workstation's operating system is Windows 2000.
- ◆ Check Point® VPN-1® is running on the workstation.

You must *always* restart the workstation after uninstalling, upgrading, or repairing the Remote Filtering Client.

---

- ◆ **REINSTALL=ALL**

This parameter is used only when repairing or upgrading an existing installation of Remote Filtering Client. It indicates the components to remove and reinstall. The value should always be set to ALL.

◆ **REINSTALLMODE=veums | voums**

This parameter is used only when repairing or upgrading an existing installation of Remote Filtering Client. It defines either a repair or an upgrade. The possible values are:

- **veums**: for repairs only
- **voums**: for upgrades only

◆ **/qn**

Switch for quiet installation mode. When you use this option, Remote Filtering Client will install without displaying information to the employee at the workstation. If you do not use **/qn**, the installer launches in interactive mode and installation dialog boxes display to the employee during installation. Most organizations choose the quiet mode, as interactive mass deployment has little value.

### *Installation Syntax*

The following is an example of the syntax to install the Remote Filtering Client on employee workstations using a third-party deployment tool. Replace the variables in angle brackets with appropriate values for your network, and type the command on a single line with no returns.

```
msiexec /i cpmclient.msi PASSPHRASE=<pass phrase for Remote  
Filtering Server> PRIMARY_WISP_ADDRESS=<external IP Address or  
FQDN of primary Remote Filtering Server>  
PRIMARY_WISP_PORT=<external port number of primary Remote  
Filtering Server> PRIMARY_INTERNAL_WISP_ADDRESS=<internal IP  
address or host name of primary Remote Filtering Server>  
PRIMARY_INTERNAL_WISP_PORT=<internal port number of primary  
Remote Filtering Server> REBOOT=<reboot parameter> /qn
```

For example, the installation command might look like this:

```
msiexec /i cpmclient.msi PASSPHRASE=2gbatfm  
PRIMARY_WISP_ADDRESS=63.16.200.232  
PRIMARY_WISP_PORT=80  
PRIMARY_INTERNAL_WISP_ADDRESS=10.218.5.60  
PRIMARY_INTERNAL_WISP_PORT=9000  
REBOOT=IF_NEEDED_PROMPT /qn
```

If you are using secondary or tertiary Remote Filtering Servers, you must enter parameters for those machines as well.

### ***Repair Syntax***

The following is an example of the syntax to repair an existing installation of Remote Filtering Client using a third-party deployment tool. This command must be typed on a single line with no returns.

```
msiexec /i cpmclient.msi REINSTALL=ALL  
REINSTALLMODE=veums /qn
```

When the installer repairs an installation of the Remote Filtering Client, the current configuration settings are used. If your remote filtering configuration *has not* changed, no additional parameters are necessary. However, if you have changed your configuration, you must include the appropriate parameters and new values in the command.



#### **Note**

For the syntax required to upgrade Remote Filtering Clients to a new version, see [Upgrading Remote Filtering Client with a Third-Party Deployment Tool](#), page 53.

---

### ***Uninstall Command***

The following is the actual command that can be used to uninstall the Remote Filtering Client with a third-party deployment tool. This command must be typed on a single line with no returns.

```
msiexec.exe /x - {14D74337-01C2-4F8F-B44B-  
67FC613E5B1F} /qn
```

## Solaris and Linux Procedures

The steps in this section are common to all installations of Websense Enterprise/Web Security Suite components on Solaris or Linux. Start here to download and run the Websense installer, and then refer to the appropriate sections for the component-specific procedures.

To install components separately on a Solaris or Linux machine:

1. Log on to the installation machine as the **root** user.
2. Close all applications and stop any antivirus software.
3. Create a setup directory for the installer files.

For example: `/root/Websense_setup`

4. Obtain an installer package for Websense Enterprise/Web Security Suite:

**Web download:** To download an installer package, go to [www.websense.com](http://www.websense.com), and then navigate to the Downloads page.

- a. Choose the dynamic (online) or full (offline) installer package, the operating system, and the language.



**Note**

The **Dynamic** installer is an **online** installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.

The **Full** installer is a complete **offline** installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install the Websense Enterprise/Web Security Suite components. Use this package if you experience difficulties with the online installer.

---

- b. Save the selected installer package to the setup directory on the installation machine.

5. In the setup directory, enter the following command to unzip the file:

```
gunzip <download file name>
```

For example: `gunzip Websense631Setup_Slr.tar.gz`

6. Expand the file into its components with the following command:

```
tar xvf <unzipped file name>
```

For example: `tar xvf Websense631Setup_Slr.tar`



This places the following files into the setup directory:

File	Description
install.sh	Installation program
Setup	Archive file containing related installation files and documents.
Documentation	Release Notes: An HTML file containing release notes and last minute information about the Websense software. Read this file with any supported browser.

7. Run the installation program from the setup directory with the following command:

```
./install.sh
```

To run the GUI version of the installer, use the following command:

```
./install.sh -g
```

If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.

8. Follow the onscreen instructions through the subscription agreement.
9. (*Web Security Suite only.*) When asked for a product selection, select the Web Security Suite edition you plan to use.

The installer displays information about the required installation sequence for the components of this product on your operating system.

10. Select **Custom** when asked what type of installation you want.
11. To continue, proceed to the appropriate component section.

## Websense Manager

Websense Manager, the administrative interface for your Websense software, can be installed in multiple locations in your network for convenient access. The Websense Manager machine needs network access to the Policy Server machine.

To install Websense Manager on a Solaris or Linux machine.

1. Download and start the installer using the procedure in *Solaris and Linux Procedures*, page 143.

2. Following the **Custom** installation path brings you to a list of components to install. Select **Websense Manager**.

The installer asks you for the location of your web browser.

3. Provide the full path to the web browser to use when viewing online Help.

The installer asks you to provide a path to the installation directory in which it can create the `/Manager` subdirectory and install Websense Manager.

4. Enter the path to the installation directory, or accept the default installation directory (`/opt/Websense`). If this directory does not already exist, the installer will create it.



### Important

The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

---

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary list appears, showing the installation path, the installation size, and the component (Websense Manager) you have selected.

5. Select **Next** to begin installing Websense Manager.
6. The Download Manager downloads the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.

If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Select **Next** to continue.

7. When a message announcing successful completion of the installation is displayed:
  - If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions.
  - If you chose an English language installer:
    - If you are installing in command line mode, select **Finish** to exit the installer.
    - If you are installing in GUI mode, select **Next** to continue. The installer asks if you want to start Websense Manager. Make a choice and select **Finish** to exit the installer.
8. If you stopped your antivirus software, remember to start it again after Websense components have been installed.



#### Note

To launch Websense Manager on a Solaris or Linux machine, go to the `/Manager` subdirectory in the Websense installation directory (by default, `opt/Websense/Manager`) and enter:

```
./start_manager
```

---

## Network Agent

You can install Network Agent on a Solaris or Linux machine separate from the Filtering Service. Network Agent must be able to monitor 2-way internet traffic from the internal network. Install Network Agent on a machine that can see the internet requests *from* the internal network as well as the internet response *to* the requesting workstations.



#### Important

If you install Network Agent on a machine that cannot monitor the targeted traffic, Network Agent features such as Protocol Management, Bandwidth Optimizer, and IM Attachment Manager will not perform as expected.

---

If this installation is part of a multiple deployment of the Network Agent (for load balancing purposes), you must be sure that the IP address ranges for each instance of the Network Agent do not overlap. This will result in double logging. Deploy the Network Agents so that they can filter the entire network. Partial deployment will result in incomplete filtering by protocol and bandwidth, as well as the loss of log data from network segments not watched by Network Agent.

To define IP address ranges for multiple Network Agents, follow the instructions in the *Administrator's Guide* for Websense Enterprise/Web Security Suite. For detailed information about deploying Network Agent, see the *Deployment Guide* for Websense Enterprise/Web Security Suite.

*Do not* install Network Agent on a machine running any type of firewall. Network Agent uses a packet capturing utility which may not work properly when installed on a firewall machine.

If you are attempting to install Network Agent on a machine on which the Filtering Service and Policy Server are already installed, see the procedures in [Adding Components](#), page 163.



### Important

The Websense Filtering Service and Policy Server must be installed and running prior to installing Network Agent, or installed at the same time as Network Agent. The installer asks for the IP addresses and port numbers of these components and will not install Network Agent if the Policy Server and Filtering Service cannot be located.

---

1. Download and start the installer using the procedure in [Solaris and Linux Procedures](#), page 143.
2. Following the **Custom** installation path brings you to a list of components to install. Select **Network Agent**.

The installer asks you to identify the machine on which the Policy Server is installed.



**Note**

The displayed configuration port (55806) is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number.

---

3. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then select **Next**.

The installer asks you if this machine is running a firewall. Make sure that the installation machine is not being used as a firewall before continuing.

---



**Important**

Network Agent cannot function properly on a machine running a firewall.

The only exception is a blade server or appliance that has separate processors or virtual processors to accommodate Network Agent and the firewall software.

---

4. Select **Yes** or **No** and then select **Next** to continue:
  - Select **Yes** if the installation machine is *not* being used as a firewall. Installation will continue.
  - Select **No** if you are attempting to install Network Agent on a firewall machine, and Setup will exit. Install Network Agent on a machine that is not running a firewall.

All enabled network interface cards (NICs) on the machine appear in a list.

5. If the machine has multiple NICs, select the one that has visibility into the internet traffic you want Network Agent to filter.
- 



**Note**

After installation, you can run the Traffic Visibility Tool to test whether the selected NIC can see the appropriate user internet traffic. See [Testing Visibility of Internet Traffic to Network Agent](#), page 204.

---

The installer asks you for the IP address and filter port number for the machine on which Filtering Service is installed.



**Note**

The displayed filter port (15868) is the default port number used by the installer to install Filtering Service. If you installed Filtering Service using a different port number, enter that port number.

---

6. Enter the IP address of the Filtering Service machine, and the port number if different from the default, and then select **Next** to continue.

The installer asks if you want to allow Websense, Inc., to gather information about the use of Websense-defined protocols. Information will be used in the development of protocol filtering.



**Note**

Network Agent never sends Websense, Inc., any information that would identify specific users, no matter which Network Agent feedback option is selected.

---

7. Select a Network Agent feedback option, and then select **Next** to continue.

The installer asks you for the location of the installation directory.

8. Enter the path to the installation directory, or accept the default Websense installation directory (`/opt/Websense`). If this directory does not already exist, the installer will create it.



**Important**

The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

---

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary of all the components that will be installed appears.

9. Select **Next** to begin installation.

The Download Manager downloads the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.

10. When a message announcing successful completion of the installation is displayed:

- If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions.
- If you chose an English language installer, select **Finish** to exit the installer.

11. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

12. Configure Network Agent for use in your network. See the instructions for initial configuration of Network Agent in *Chapter 5: Initial Setup*, as well as the Network Agent chapter in the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

## RADIUS Agent

The Websense RADIUS Agent allows you to integrate your Websense filtering policies with authentication provided by a RADIUS server. The RADIUS Agent enables Websense software to transparently identify users who access your network using a dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), or other remote connection.

To install the RADIUS Agent on a Solaris or Linux machine:

1. Download and start the installer using the procedure in *Solaris and Linux Procedures*, page 143.
2. Following the **Custom** installation path brings you to a list of components to install. Select **RADIUS Agent**.

If the installation machine is multihomed, all enabled network interface cards (NICs) with an IP address are displayed.

3. Select the IP address of the card you want RADIUS Agent to use to communicate.

The installer asks you to identify the machine on which the Policy Server is installed.



#### Note

The displayed configuration port (55806) is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number.

---

4. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then select **Next** to continue.

The installer asks you for the location of the installation directory.

5. Enter the path to the installation directory, or accept the default Websense installation directory (`/opt/Websense`). If this directory does not already exist, the installer will create it.



#### Important

The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

---

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary of all the components that will be installed appears.



6. Select **Next** to begin installation.

The Download Manager downloads the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.

If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Select **Next** to continue.
7. When a message announcing successful completion of the installation is displayed:
  - If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions.
  - If you chose an English language installer, select **Finish** to exit the installer.
8. If you stopped your antivirus software, remember to start it again after Websense components have been installed.
9. Configure the RADIUS Agent, and configure your environment for RADIUS Agent. For instructions, see the User Identification chapter in the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

## eDirectory Agent

The Websense eDirectory Agent works together with Novell eDirectory to identify users transparently so that Websense software can filter requests according to particular policies assigned to users or groups.

Do not install eDirectory Agent on the same machine as DC Agent or Logon Agent, as this can cause conflicts.

To install the eDirectory Agent on a Solaris or Linux machine:

1. Download and start the installer using the procedure in *Solaris and Linux Procedures*, page 143.
2. Following the **Custom** installation path brings you to a list of components to install. Select **eDirectory Agent**.

The installer asks you to identify the machine on which the Policy Server is installed.



**Note**

The displayed configuration port (55806) is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number.

---

3. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then select **Next** to continue.

If the installation machine is multihomed, all enabled network interface cards (NICs) with an IP address are displayed.

4. Select the IP address of the card you want eDirectory Agent to use to communicate, and then select **Next** to continue.

The installer asks for the Novell eDirectory name and password.

5. Enter the full *distinguished name* and a valid password, and then select **Next** to continue.

The installer asks you for the location of the installation directory.

6. Enter the path to the installation directory, or accept the default Websense installation directory (`/opt/Websense`). If this directory does not already exist, the installer will create it.



**Important**

The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

---

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance

of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary of all the components that will be installed appears.

7. Select **Next** to begin installation.

The Download Manager downloads the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.

If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Select **Next** to continue.

8. When a message announcing successful completion of the installation is displayed:
  - If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions.
  - If you chose an English language installer, select **Finish** to exit the installer.
9. If you stopped your antivirus software, remember to start it again after Websense components have been installed.
10. Configure the eDirectory Agent and Novell eDirectory by following the instructions in the User Identification chapter of the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

## Logon Agent

Logon Agent is a Websense transparent identification agent that detects users as they log on to Windows domains in your network via client machines. The Logon Agent receives logon information from `LogonApp.exe`, a separate client application that runs only on Windows client machines, and must be run by a logon script. For information about setting up this script in your network, see [Creating and Running the Script for Logon Agent](#), page 196.

Logon Agent can be run together with DC Agent if some of the users in your network are not being authenticated properly. This might happen if your network uses Windows 98 workstations, which do not permit DC Agent to poll users for their identification when they make an internet request.

Do not install Logon Agent on the same machine as eDirectory Agent, as this can cause conflicts.

To install the Logon Agent on a Solaris or Linux machine:



**Note**

LogonApp.exe, the client application that passes user logon information to Logon Agent, runs only on Windows client machines.

---

1. Download and start the installer using the procedure in *Solaris and Linux Procedures*, page 143.
2. Following the **Custom** installation path brings you to the component selection screen. Select **Logon Agent**.

The installer asks you to identify the machine on which the Policy Server is installed.



**Note**

The displayed configuration port (55806) is the default port number used by the installer to install the Policy Server. If you installed the Policy Server using a different port number, enter that port number.

---

3. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then select **Next** to continue.

If the installation machine is multihomed, all enabled network interface cards (NICs) with an IP address appear in a list.

4. Select the IP address of the card you want Logon Agent to use to communicate.

The installer asks you for the location of the installation directory.

5. Enter the path to the installation directory, or accept the default Websense installation directory (`/opt/Websense`). If this directory does not already exist, the installer will create it.



### Important

The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

---

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary of all the components that will be installed appears.

6. Select **Next** to begin installation.

The Download Manager downloads the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.

If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Select **Next** to continue.

7. When a message announcing successful completion of the installation is displayed:
  - If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions.
  - If you chose an English language installer, select **Finish** to exit the installer.
8. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

9. Set up the required logon script by following the instructions in [Creating and Running the Script for Logon Agent](#), page 196.
10. Configure Logon Agent to communicate with client workstations and the Filtering Service by following the instructions in the User Identification chapter of the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

## Remote Filtering Server

The Remote Filtering Server provides web filtering for user workstations located outside the network firewall. In order to be filtered through the Remote Filtering Server, a remote workstation must be running the Remote Filtering Client. (For Remote Filtering Client installation instructions, see [Remote Filtering Client](#), page 132.)



### Note

To enable the Remote Filtering components, you must subscribe to the remote filtering service.

---

The Remote Filtering Server should be installed on a separate, dedicated machine. This machine must be able to communicate with the Websense Filtering Service and with the remote workstations outside the network firewall. The Remote Filtering Server machine does not have to be joined to a domain.

The Remote Filtering Server should be installed inside your organization's outermost network firewall, but in the DMZ outside the firewall that protects the rest of the corporate network. For more information about deploying the Remote Filtering Server in your network, see the *Remote Filtering* section in the *Deployment Guide* for Websense Enterprise/Web Security Suite.

To provide failover capability for the primary Remote Filtering Server, you can install secondary and tertiary Remote Filtering Servers. Each Remote Filtering Client can be configured to connect with a primary, secondary, and tertiary Remote Filtering Server. If the primary server is unavailable, the

client attempts to connect with the secondary, then the tertiary, then the primary again, and so on.



### Important

- ◆ Install only one primary Remote Filtering Server for each Filtering Service in your network.
  - ◆ Do not install the Remote Filtering Server on the same machine as the Filtering Service or Network Agent.
  - ◆ Do not enable DHCP on the Remote Filtering Server machine.
- 

To install the Remote Filtering Server on a Solaris or Linux machine:

1. Download and start the installer using the procedure in [Solaris and Linux Procedures](#), page 143.
2. Following the **Custom** installation path brings you to a list of components to install. Select **Remote Filtering Server**.

If the installation machine is multihomed, all enabled network interface cards (NICs) with an IP address are displayed.

3. Select the IP address of the card you want the Remote Filtering Server to use to communicate with other Websense components inside the network firewall, and then select **Next** to continue.

Remote Filtering Clients must be able to connect to the Remote Filtering Server, both from inside and from outside the internet gateway or network firewall. The installer asks you to provide connection information for this machine.

4. In the **External IP Address or Host Name** field, enter an IP address or machine name (in the form of a fully qualified domain name) that is visible from *outside* the firewall.

5. In the **External Communication Port** field, enter a port number (from 10 to 65535) that is not in use, and that is accessible from *outside* the network firewall. The default value is 80. (If there is a web server installed on the machine, port 80 may already be in use, so you may need to change the default value.)



### Important

The port entered as the **External Communication Port** must be opened on your network firewall to accept connections from Remote Filtering Clients on workstations located outside the firewall. For more information, see [Firewall Configuration for Remote Filtering](#), page 209.

---

6. In the **Internal Communication Port** field, enter a port number (from 1024 to 65535) that is not in use, and that is accessible only from *inside* the network firewall. The default value is 8800.



### Important

Be sure that your network firewall is configured to block connections to the **Internal Communication Port** from workstations located outside the firewall. For more information, see [Firewall Configuration for Remote Filtering](#), page 209.

---

The installer asks you to enter a pass phrase of any length for the Remote Filtering Server. This pass phrase will be combined with unpublished keys to create an encrypted authentication key (shared secret) for secure client/server communication.

7. Before selecting a **pass phrase**, consider the following requirements:
  - If Websense Client Policy Manager (CPM) is already installed in your network, you must enter the same pass phrase used when installing CPM.
  - If you install Websense Client Policy Manager (CPM) in your network in the future, you must use the pass phrase you enter in this screen.



- If you want this installation of the Remote Filtering Server to function as a backup (secondary or tertiary) server for a primary Remote Filtering Server, you must enter the same pass phrase used when installing the primary Remote Filtering Server.
- The pass phrase must include only ASCII characters. Do not use extended ASCII or double-byte characters.
- You must use the pass phrase you enter in this screen when you install the Remote Filtering Clients that will connect with this server. (See [Remote Filtering Server Connection Information](#), page 135.)



### Warning

Be sure to record your **pass phrase** and keep it in a safe place, as it cannot be retrieved from the Websense system later.

---

8. Enter and confirm your **pass phrase**.  
The installer asks you to provide information about the machine on which the Websense Filtering Service is installed.
9. Enter the actual (internal) IP address of the Filtering Service machine.  
The installer asks if there is a firewall or other network device that performs network address translation between the Filtering Service machine and this Remote Filtering Server machine.
10. Enter **yes** or **no**.  
If you entered **yes**, the installer asks for the translated (external) IP address of the Filtering Service machine, visible to this machine. Enter the translated IP address.
11. Enter the filter port number for the Filtering Service machine, if it was changed from the default of 15868.



### Note

The filter port is the default communication port used by the installer to install Filtering Service. If you installed Filtering Service using a different communication port, enter that port number.

---

12. Enter the block page port number for the Filtering Service machine, if it was changed from the default value of 15871.



### Important

If there is a firewall between the Filtering Service machine and the Remote Filtering Server machine, be sure to open the filter port (15868) and block page port (15871) on that firewall. Filtering Service must be able to accept connections from the Remote Filtering Server, and serve block pages to remote users. For more information, see [Firewall Configuration for Remote Filtering, page 209](#).

---

The installer asks you for the location of the installation directory.

13. Enter the path to the installation directory, or accept the default Websense installation directory (`/opt/Websense`). If this directory does not already exist, the installer will create it.



### Important

The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

---

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary of all the components that will be installed appears.

14. Select **Next** to begin installation.

The Download Manager downloads the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.

Since the Network Agent was not installed on this machine, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Select **Next** to continue.

15. When a message announcing successful completion of the installation is displayed:
  - If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions.
  - If you chose an English language installer, select **Finish** to exit the installer.
16. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

For more information about how remote filtering works, see the *Filtering Remote Clients* section in the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

## Modifying an Installation

---

If you decide to change the location of a Websense component or modify your Websense installation, run the installer again on the machine you want to modify and select the appropriate option. The installer detects the presence of Websense components and offers you the following installation options:

- ◆ Add Websense components.
- ◆ Remove Websense components.
- ◆ Repair existing Websense components.

## Adding Components

After installing Websense Enterprise/Web Security Suite, you may want to add components to change the configuration of Websense software in your network. The following procedures assume that the Filtering Service, Policy Server, User Service, Usage Monitor, and Websense Manager are already installed, and that additional components are going to be added. If you are adding remote components, the installer will ask you for the location of the Policy Server.

## Windows

To add Websense components in a Windows environment:



### Note

Before adding new components, we recommend that you perform a full system backup as a fallback strategy. This backup allows you to restore your current system with minimum downtime, should you decide to do so.

---

1. Log on to the installation machine with **domain** and **local** administrator privileges.

If you are adding User Service or DC Agent, this will assure that they have administrator privileges on the domain.



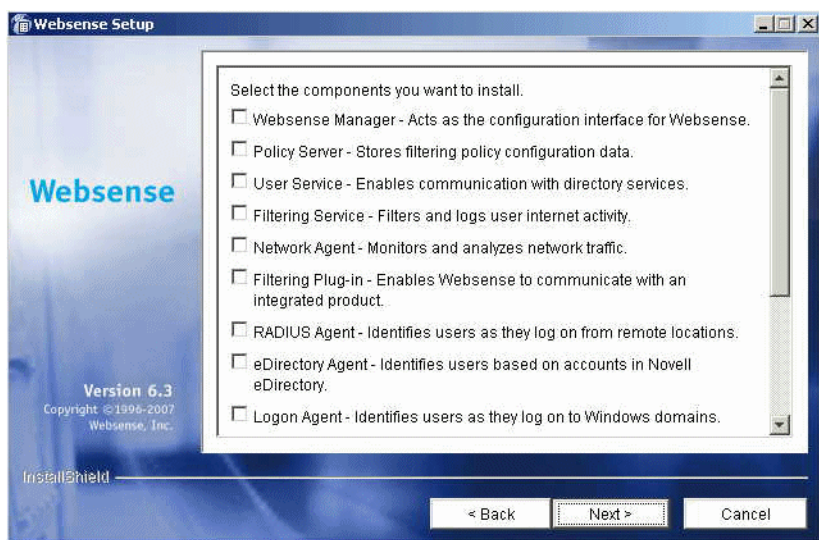
### Important

User Service and DC Agent must have administrator privileges on the network to retrieve user login information from the domain controller. Without this information, Websense software cannot filter by users and groups. If you cannot install these components with such privileges, you can configure domain administrator privileges for these services after installation. For instructions, see [Configure Domain Administrator Privileges, page 207](#).

---

2. Close all applications and stop any antivirus software.
3. Go to the folder where you extracted the Windows Websense installer files, and double-click `Setup.exe` to launch the installer.
4. Click **Next** in the welcome screen.  
A dialog box appears asking you what action you want to take with the Websense components the installer has detected on the machine.
5. Select **Add Websense components** and click **Next**.

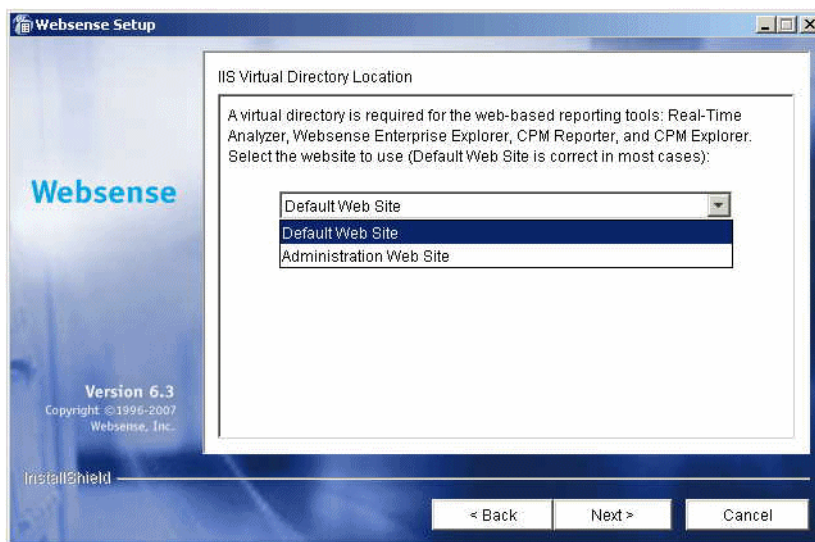
The installer displays a list of components not currently installed on the installation machine.



Websense Component Selection

6. Select the components you want to install and click **Next**.

If you are installing the Real-Time Analyzer and are using IIS as your web server, you are prompted to select the name of the website in the IIS Manager under which the installer should create a *virtual directory*. The default value is **Default Web Site**, which is correct in most instances.



Virtual Directory Selection

7. If you have renamed the default website in the IIS Manager or are using a language version of Windows other than English, select the proper website from the names in the drop-down list, and then click **Next** to continue.

If you are installing Network Agent, the installer asks you if this machine is running a firewall. Network Agent cannot function properly on a machine that is being used as a firewall. (The only exception is a blade server or appliance that has separate processors or virtual processors to accommodate Websense software and the firewall software.)

8. Select **Yes** or **No** and click **Next** to continue:
  - Select **Yes** if the installation machine is *not* being used as a firewall. Installation will continue.
  - Select **No** if you are attempting to install Network Agent on a firewall machine, and Setup will exit. Install Network Agent on a machine that is not running a firewall.



### Important

The machine on which Network Agent is installed must be able to monitor 2-way employee internet traffic to function correctly. If you install Network Agent on a machine that cannot monitor the targeted traffic, Network Agent features such as Protocol Management, Bandwidth Optimizer, and IM Attachment Manager will not perform as expected.

---

If you are installing Network Agent, a screen appears asking you to select the network interface card (NIC) that you want Network Agent to use for capturing traffic. All network interface cards enabled in the machine appear in a list.

9. If the machine has multiple NICs, select the one that has visibility into the internet traffic you want Network Agent to filter.



### Note

After installation, you can run the Traffic Visibility Tool to test whether the selected NIC can see the appropriate user internet traffic. See *Testing Visibility of Internet Traffic to Network Agent*, page 204.

---

10. Click **Next** to continue.

If you are installing Network Agent, a screen appears asking if you want to allow Websense, Inc., to gather information about the use of Websense-defined protocols. Information will be used in the development of protocol filtering.



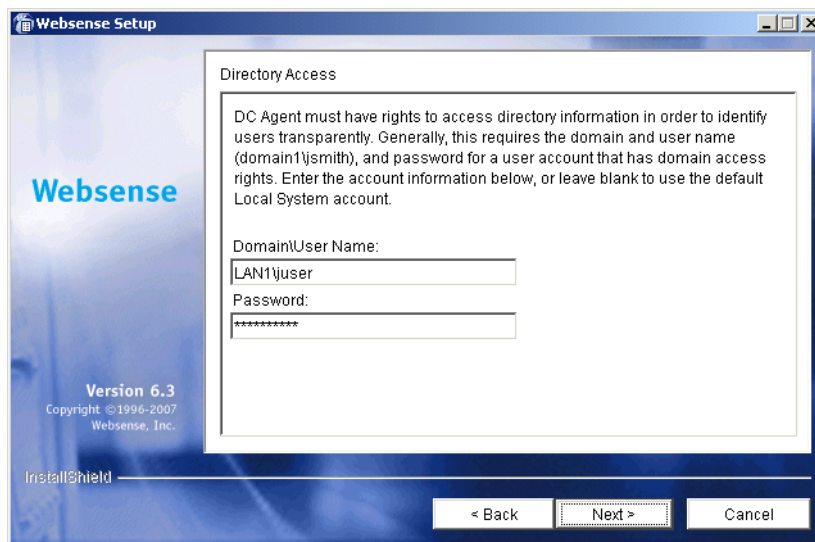
### Note

Network Agent never sends Websense, Inc., any information that would identify specific users, no matter which Network Agent feedback option is selected.

---

11. Select a Network Agent feedback option and click **Next** to continue.

If you selected DC Agent for installation, you are asked to provide a user name and a password with administrative privileges on the domain. DC Agent needs access to directory information to be able to identify users transparently.



Directory Access for DC Agent

12. Enter the domain and user name, followed by the network password for an account with domain privileges, and click **Next** to continue.



**Note**

If you cannot install DC Agent with the appropriate privileges, you can configure domain administrator privileges for it after installation. For instructions, see [Configure Domain Administrator Privileges, page 207](#).

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance



of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A summary screen appears, listing the installation path, the installation size, and the components that will be installed.

13. Click **Next** to begin installation.

The Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

If Network Agent was *not* installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

14. When a message announcing successful completion of the installation is displayed:

- If you chose a non-English language installer, the Websense Language Pack installer starts.

Click **Next** in the welcome screen and follow the onscreen instructions to update Websense components with text in the selected language.

- If you chose an English language installer:
  - If Websense Manager was not installed, click **Finish** to exit the installer.
  - If Websense Manager was installed, click **Next** to continue.

The installer displays a screen asking if you want to launch Websense Manager. If you do not want to launch Manager, clear the checkbox. Click **Finish** to exit the installer.



#### **Note**

Before you can access Real-Time Analyzer and other Websense Reporting Tools, you must first log on to Websense Manager and configure user permissions. For more information, see the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

---

15. If you stopped your antivirus software, be sure to start it again.

## Solaris or Linux

To add Websense Enterprise/Web Security Suite components in a Solaris or Linux environment:



---

### Note

Before adding new components, we recommend that you perform a full system backup as a fallback strategy. This will allow you to restore your current system with a minimum of downtime, should you decide to do so.

---

1. Log on to the installation machine as the **root** user.
2. Close all applications and stop any antivirus software.
3. Run the installation program from the directory where it resides using the following command:

```
./install.sh
```

To run the GUI version of the installer, use the following command:

```
./install.sh -g
```

If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.

The installer detects the currently installed Websense components and asks you what action you want to take.

4. Select **Add Websense components**.  
The installer asks you to select the components that you want to install. The installer displays a list of components not currently installed on the installation machine.
5. Select the components you want to install, and then select **Next** to continue.
6. Make the following selections during installation:
  - **Firewall installation warning:** If you are installing Network Agent, the installer displays a warning that Network Agent cannot function properly on a machine running a firewall. (The only exception is a blade server or appliance that has separate processors or virtual processors to accommodate Websense software and the firewall software.)

Select **Yes** or **No** when asked if you want to install Network Agent:

- Select **Yes** if the installation machine is *not* being used as a firewall. Installation will continue.
- Select **No** if you are attempting to install Network Agent on a firewall machine, and Setup will exit. Install Network Agent on a machine that is not running a firewall.



### Important

The machine on which Network Agent is installed must be able to monitor 2-way employee internet traffic to function correctly. If you install Network Agent on a machine that cannot monitor the targeted traffic, Network Agent features such as Protocol Management, Bandwidth Optimizer, and IM Attachment Manager will not perform as expected.

---

- **Network Interface Card (NIC) selection:** If you are installing Network Agent, all enabled network interface cards (NICs) appear in a list. If the machine has multiple NICs, select the one to use for Network Agent. Be sure that this card has visibility into the internet traffic you want Network Agent to filter.



### Note

After installation, you can run the Traffic Visibility Tool to test whether the selected NIC can see the appropriate user internet traffic. See [Testing Visibility of Internet Traffic to Network Agent](#), page 204.

---

- **Network Agent Feedback:** If you are installing Network Agent, the installer asks if you want to allow Websense, Inc., to gather information about the use of Websense-defined protocols. Information will be used in the development of protocol filtering. Select a Network Agent feedback option and continue.



### Note

Network Agent never sends Websense, Inc., any information that would identify specific users, no matter which Network Agent feedback option is selected.

---

- **System requirements check:** The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.
    - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
    - If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.
  - **Installation summary:** A summary list appears, showing the installation path, the installation size, and the components that will be installed.
7. Select **Next** to begin installing the displayed Websense components.
- The Download Manager downloads the appropriate installer files from the Websense website. Installation begins automatically when the necessary files have been downloaded.
- If Network Agent was not installed, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Select **Next** to continue.
8. When a message announcing successful completion of the installation is displayed:
- If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions to update Websense components with text in the selected language.
  - If you chose an English language installer:
    - If you are installing in command line mode, or if you are installing in GUI mode and did not install Websense Manager, select **Finish** to exit the installer.
    - If you are installing in GUI mode and you installed Websense Manager, select **Next** to continue. The installer asks if you want to start Websense Manager. Make a choice and select **Finish** to exit the installer.
9. If you stopped your antivirus software, be sure to start it again.

## Removing Components

After installing Websense Enterprise/Web Security Suite or any of their components, you may want to remove components to change the configuration of Websense software in your network.



### Important

The Policy Server service must be running to uninstall any Websense components. To remove the Policy Server, you must also remove all the other components installed on the machine.

---

## Windows

To remove installed Websense Enterprise/Web Security Suite components in a Windows environment:



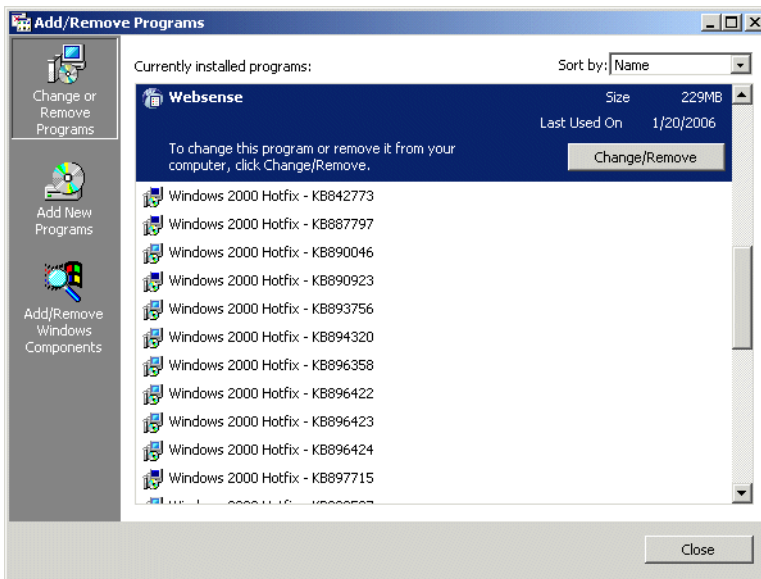
### Note

Before removing components, we recommend that you perform a full system backup as a fallback strategy.

---

1. Log on to the installation machine with **local** administrator privileges.
2. Close all applications and stop any antivirus software.
3. Go to the Windows Add or Remove Programs dialog box:
  - *Windows Server 2003*: Select **Start > Control Panel > Add or Remove Programs**.
  - *Windows 2000*: Select **Start > Settings > Control Panel**, and then double-click **Add/Remove Programs**.

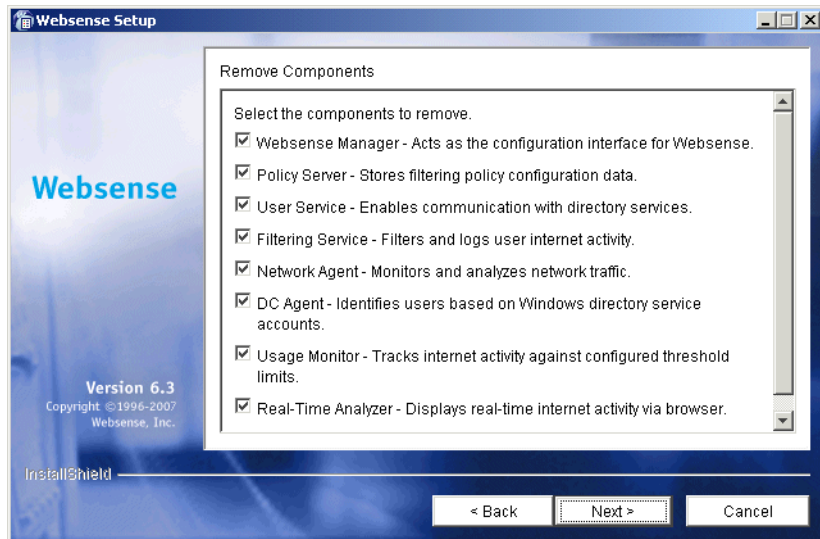
4. Select **Websense** from the list of installed applications.



Add/Remove Programs Control Panel, Windows 2000

5. Click **Change/Remove** to launch the Websense uninstaller.  
There may be a delay of several seconds while the Websense uninstaller starts.

A list of installed components appears.



### Remove Components

By default, all components are checked for removal.



#### Warning

Do not uninstall the Policy Server without uninstalling all of the Websense components. Removing the Policy Server will sever communication with the remaining Websense components and will require the reinstallation of those components.

- To keep a component, remove the check mark from the box next to it. When all of the components you want to uninstall are checked, click **Next** to continue.



#### Note

If you are uninstalling Filtering Service, make sure that all associated Network Agents are uninstalled. If you try to uninstall Network Agent *after* its associated Filtering Service has been removed, the installer will be unable to stop Network Agent and will display an error message.

If the Policy Server is not running, a dialog box appears advising you that removing Websense components may require communication with the Policy Server. You may exit the installer to restart the Policy Server, or continue uninstalling the selected components.



### Warning

If the Policy Server is not running, the files for the selected components will be removed, but not the information about the components recorded in the `config.xml` file. This could cause problems if you decide to add these components again at a later date.

---

A summary list of the components you have selected to remove appears.

7. Click **Next** to begin uninstalling the components.

If you are uninstalling Network Agent on a remote machine after removing the Policy Server, expect the process to take several minutes. Network Agent will be successfully uninstalled, although no progress notification will be displayed.

A completion messages advises you when the procedure is finished.

8. Click **Next** to continue.

A dialog box appears advising you that the machine must be restarted to complete the uninstall process.

9. Select a restart option and click **Finish** to exit the installer.
10. If you stopped your antivirus software, be sure to start it again.

## Solaris or Linux

To remove installed components on a Solaris or Linux machine:



### Note

Before removing components, we recommend that you perform a full system backup as a fallback strategy.

---

1. Log on to the installation machine as the **root** user.
2. Close all applications and stop any antivirus software.



3. Run the following program from the Websense installation directory (default is `/opt/Websense`):

```
./uninstall.sh
```

Run the GUI version of the installer with the following command:

```
./uninstall.sh -g
```

If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.

The installer detects the currently installed Websense components and displays a list of installed components. By default, all components are selected for removal.



### Warning

Do not uninstall the Policy Server without uninstalling all of the Websense components. Removing the Policy Server will sever communication with the remaining Websense components and will require the reinstallation of those components.

---

4. Make sure that only the components you want to remove are selected, and then select **Next** to continue.
  - **Policy Server status:** If the Policy Server is not running, a dialog box appears advising you that removing Websense components may require communication with the Policy Server. You may exit the installer to restart the Policy Server, or continue uninstalling the selected components.



### Warning

If the Policy Server is not running, the files for the selected components will be removed, but not the information about the components recorded in the `config.xml` file. This could cause problems if you decide to add these components again at a later date.

---

- **Summary list:** A summary list of the components you have selected to remove appears. Select **Next** to remove these components.

- **Network Agent:** If you are uninstalling Network Agent on a remote machine after removing the Policy Server, expect the process to take several minutes. Network Agent will be successfully uninstalled, although no progress notification will be displayed.
  - **Completion:** A completion message advises you when the procedure is finished.
5. Exit the installer.
  6. If you stopped your antivirus software, be sure to start it again.

## Repairing an Installation

If a component fails to install properly, or is not performing normally, you can run the Websense installer again and *repair* the installation. This procedure does not troubleshoot components, but merely replaces missing files.



### Note

To repair (reinstall) a Policy Server in a distributed environment, see [Repairing the Policy Server](#), page 183 for instructions.

---

## Windows

To repair your Websense Enterprise/Web Security Suite installation in a Windows environment:



### Note

Before repairing components, we recommend that you perform a full system backup as a fallback strategy.

---

1. Log on to the installation machine with **domain** and **local** administrator privileges.  
If you are repairing User Service or DC Agent, this will assure that they have administrator privileges on the domain.



### Important

User Service and DC Agent must have administrator privileges on the network to retrieve user login information from the domain controller. Without this information, Websense software cannot filter by users and groups. If you cannot install these components with such privileges, you can configure domain administrator privileges for these services after installation. For instructions, see [Configure Domain Administrator Privileges, page 207](#).

---

2. Back up the following files to a safe location:
  - config.xml
  - websense.ini
  - eimserver.ini
3. Close all applications and stop any antivirus software.



### Warning

Be sure to close the Windows Event Viewer, or the repair may fail.

---

4. Run the Websense Enterprise/Web Security Suite installer.
5. Click **Next** in the welcome screen.

The installer detects the current Websense installation and asks if you want to add, remove, or repair components.
6. Select **Repair existing Websense components** and click **Next**.

The installer advises you that it will repair the current installation by reinstalling the existing Websense components and asks if you want to continue.
7. Select **Yes** and click **Next**.

A list of currently running Websense services appears. The message explains that the installer will stop these services before installation.
8. Click **Next** to begin installation.

The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

- If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.

A progress message appears while the installer shuts down Websense services.

The Download Manager progress bars are displayed as the appropriate installer files are downloaded from the Websense website. Installation begins automatically when the necessary files have been downloaded.

9. If you are repairing Filtering Service, the installer asks if you want to download the Websense Master Database now or at a later time using Websense Manager. Select a database download option and click **Next**.



### Warning

During repair of the Filtering Service, the installer removes the existing Master Database. Websense filtering cannot resume until the new Master Database has been successfully downloaded, decompressed, and loaded. This may take a few minutes or more than 60 minutes, depending on factors such as internet connection speed, bandwidth, available memory, and free disk space.

---

If you have chosen to download the Master Database now, a progress bar appears. The database must first be downloaded from the internet, and then decompressed and loaded into local memory. Downloading the database from the internet can take a few minutes or more than 30 minutes, depending on factors such as internet connectivity, bandwidth, time of day, and your location relative to the download server. Decompressing and loading the database can take a few minutes or more than 30 minutes, depending on factors such as available memory, free disk space, and server process utilization.

When the database has finished loading, a message appears advising you of the status of the download. Click **Next** to continue.

10. When a message announcing successful completion of the installation is displayed:
  - If you chose a non-English language installer, click **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions to update Websense components with text in the selected language.
  - If you chose an English language installer:
    - If Websense Manager was not repaired, no further action is required and you can click **Finish** to exit the installer.
    - If Websense Manager was repaired, click **Next** to continue. The installer displays a screen asking if you want to launch Websense Manager. If you do not want to launch Manager, clear the checkbox. Click **Finish** to exit the installer.
11. If you stopped your antivirus software, be sure to start it again.

## Solaris or Linux

To repair Websense Enterprise/Web Security Suite components on a Solaris or Linux machine:



### Note

Before repairing components, we recommend that you perform a full system backup as a fallback strategy.

---

1. Log on to the installation machine as the **root** user.
2. Close all applications and stop any antivirus software.
3. Run the installation program from the directory where it resides by entering the following command:

```
./install.sh
```

To run the GUI version of the installer, use the following command:

```
./install.sh -g
```

If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.

The installer detects the currently installed Websense components and asks you what action you want to take.

4. Select **Repair existing Websense components**, and select **Next** to advance through the procedure.
  - **Repair components:** The installer advises you that it will repair the current installation by reinstalling the existing Websense components.
  - **Websense services:** A list of currently running Websense services appears. The message explains that the installer will stop these services before continuing with the installation.
  - **Web browser:** If you are repairing Websense Manager, the installer prompts you for the location of the browser.
  - **System requirements check:** The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.
    - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
    - If the installation machine has less than the recommended amount of memory, the installation will continue. To ensure the best performance of the components you are installing, you should upgrade your machine's memory to the recommended amount.
  - **Services restarted:** The Websense services are restarted after the files are reinstalled.
  - **Master Database Download:** If you are repairing Filtering Service, the installer asks if you want to download the Websense Master Database now or at a later time using Websense Manager. Select a database download option and then select **Next** to continue.



### Warning

During repair of the Filtering Service, the installer removes the existing Master Database. Websense filtering cannot resume until the new Master Database has been successfully downloaded, decompressed, and loaded. This may take a few minutes or more than 60 minutes, depending on factors such as internet connection speed, bandwidth, available memory, and free disk space.

---

If you have chosen to download the Master Database now, the download begins. The database must first be downloaded from the internet, and then decompressed and loaded into local memory. Downloading the database from the internet can take a few minutes or more than 30 minutes, depending on factors such as internet connectivity, bandwidth, time of day, and your location relative to the download server. Decompressing and loading the database can take a few minutes or more than 30 minutes, depending on factors such as available memory, free disk space, and server process utilization.

When the database has finished loading, a message appears advising you of the status of the download. Select **Next** to continue.

5. When a message announcing successful completion of the installation is displayed:
  - If you chose a non-English language installer, select **Next** to continue. The Websense Language Pack installer starts. Follow the onscreen instructions to update Websense components with text in the selected language.
  - If you chose an English language installer:
    - If you are installing in GUI mode, and Websense Manager was repaired, select **Next** to continue. The installer asks if you want to start Websense Manager. Make a choice and select **Finish** to exit the installer.
    - Otherwise, select **Finish** to exit the installer.
6. If you stopped your antivirus software, be sure to start it again.

## Repairing the Policy Server

---

It may become necessary to repair (reinstall) the Policy Server in a distributed environment. Unless this is done correctly, communication with components installed on separate machines will be broken.

To repair the Policy Server and preserve the connection between distributed components:



### Note

Before repairing components, we recommend that you perform a full system backup as a fallback strategy.

---

1. Stop the Policy Server. For instructions, see *Stopping or Starting Websense Services*, page 185.
2. Make a backup copy of the `config.xml` file and put it in a safe location.



**Note**

If you cannot make a backup copy of the current configuration file due to a system crash or other hardware problems, you can use the most recent backup copy of the file saved to a shared network drive to restore the system.

---

3. Restart the Policy Server.
4. Stop the services of the distributed Websense components on the individual machines. For instructions, see *Stopping or Starting Websense Services*, page 185.
5. Close all applications on the Policy Server machine, and stop any antivirus software.
6. Run the Websense installer on the Policy Server machine.  
The installer detects installed Websense components and asks you what action you want to take.
7. Select **Repair existing Websense components** when prompted.  
For specific instructions, see *Repairing an Installation*, page 178.
8. When the installer is finished repairing the system, exit the installer and stop the newly installed Policy Server.
9. Replace the `config.xml` file created by the repair procedure with your backup copy.
10. Restart the Policy Server.
11. If you stopped your antivirus software, be sure to start it again.
12. Restart the services of the Websense components on other machines.
13. Use Websense Manager to reload the Websense Master Database.



## Migrating between FireWall-1 Versions After Installation

---

If you plan to upgrade your FireWall-1 installation, you may do so after you install Websense Enterprise or Web Security Suite v6.3.1 without any additional modifications to your Websense system. See your Check Point documentation for information about upgrading FireWall-1.

See *Chapter 7: Configuring FireWall-1 NG, NG with AI, and NGX* for the necessary configuration procedures to ensure that your new version of FireWall-1 can communicate with Websense Enterprise or Web Security Suite v6.3.

## Stopping or Starting Websense Services

---

By default, Websense services are configured to start automatically when the computer is started.

Occasionally you may need to stop or start a Websense service. For example, you must stop the Filtering Service whenever you edit the `websense.ini` file, and after customizing default block messages.



### Note

When Filtering Service is started, CPU usage can be 90% or more for several minutes while the Websense Master Database is loaded into local memory.

---

## Manually Stopping Services

Certain Websense components must be stopped and started in a prescribed order. Optional components may be stopped and started in any order.

### Optional Components

You can manually start or stop these Websense services in any order.

- ◆ eDirectory
- ◆ RADIUS Agent

- ◆ DC Agent
- ◆ Real-Time Analyzer
- ◆ Logon Agent
- ◆ Usage Monitor
- ◆ Remote Filtering Server

## Principal Components

The following list is the preferred order for stopping the components. Start or stop optional components before stopping the components on this list. Policy Server should always be stopped last.

1. Network Agent
2. Filtering Service
3. User Service
4. Policy Server

When restarting Websense services, reverse the order, starting with the Policy Server first. In Linux and Solaris, a command stops and starts components in the proper order.

## UFP Server

The Websense Filtering Service must be running for the Websense UFP Server to function. When the Filtering Service is stopped, the UFP Server is automatically shut down. The UFP Server must be restarted manually, however, and if started first, will automatically start the Filtering Service. Stopping or starting the UFP Server while the Filtering Service is running has no effect on the Filtering Service.

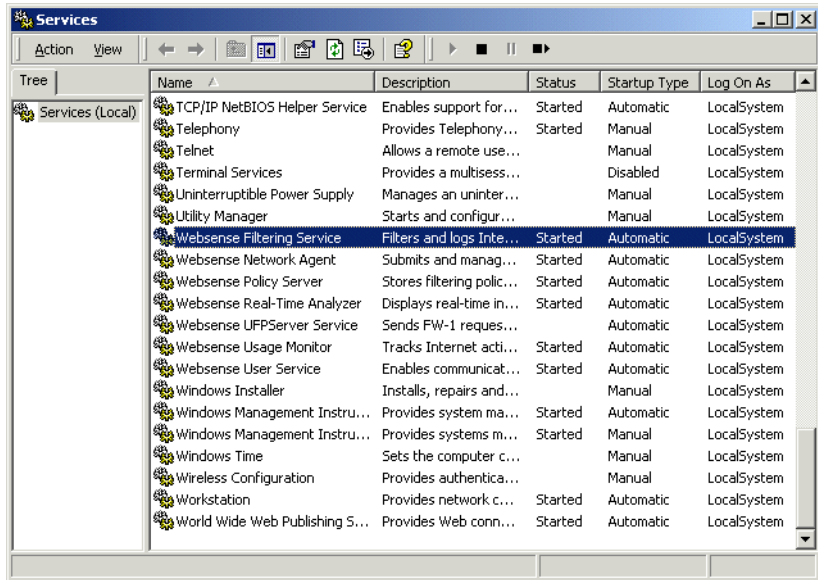
## Windows

Stop, start, or restart a Websense service by using the **Services** dialog box. Restarting stops the service, then restarts it again immediately from a single command.

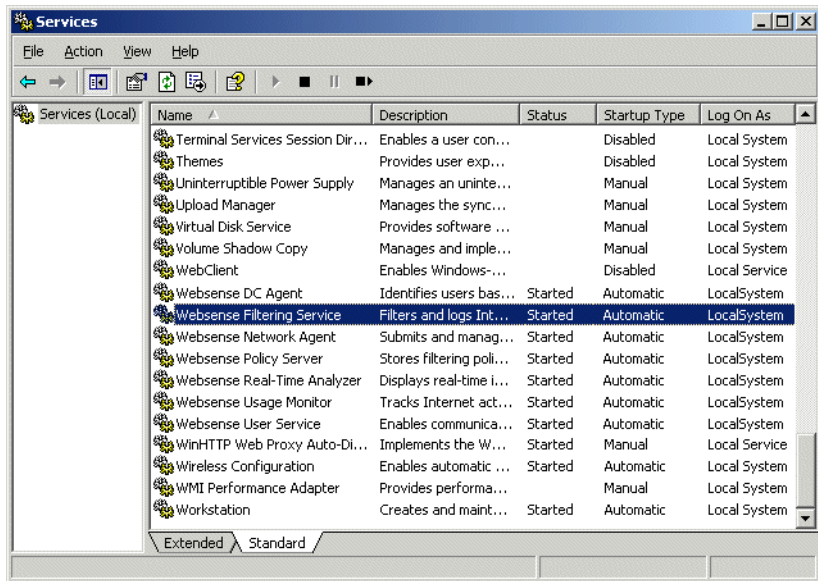
To stop or start Websense services on a Windows machine:

1. From the **Control Panel**, select **Administrative Tools > Services**.

2. Scroll down the list of available services and select a Websense service.



Windows 2000 Services List



Windows Server 2003 Services List

3. From the **Action** menu, select **Start**, **Stop**, or **Restart** or click one of the control buttons in the toolbar (**Stop** ■, **Start** ►, or **Restart** ■ ►). **Restart** stops the service, then restarts it again immediately from a single command.



### **Warning**

DO NOT use the `taskkill` command to stop Websense services. This procedure may corrupt the services.

---

## Solaris and Linux

You can stop, start, or restart Websense services on a machine from a command line on a Solaris or Linux machine. Restarting stops the services, then restarts them again immediately from a single command. If the components are spread across multiple machines, be sure that Policy Server is stopped last and started first. See [Principal Components](#), page 186 for the preferred stopping and starting order.

1. Go to the `/websense` directory.
2. Use the following commands to stop, start, or restart all Websense services in the correct order:
  - `./WebsenseAdmin stop`
  - `./WebsenseAdmin start`
  - `./WebsenseAdmin restart`
3. View the running status of all Websense services with the following command:

```
./WebsenseAdmin status
```



### **Warning**

DO NOT use the `kill -9` command to stop Websense services. This procedure may corrupt the services.

---

This chapter provides initial setup and configuration procedures for preparing your Websense software to communicate with Check Point FireWall-1.

After installing the Websense software and your integration product, perform the following tasks to complete the setup process.

- ◆ If you did not download the Websense Master Database during installation, use Websense Manager and your Websense subscription key to download the database. See *Subscription Key and Master Database Download*, page 190 for instructions.
- ◆ If the Filtering Service is installed on a multihomed machine, identify the Filtering Service by its IP address in your network so that Websense block messages can be sent to users. See *Identifying the Filtering Service for the Block Page URL*, page 194 for instructions.
- ◆ All Windows workstations being filtered must have the Messenger Service enabled to receive protocol block messages. See *Displaying Protocol Block Messages*, page 195 for instructions.
- ◆ If the Logon Agent was installed, you must create a logon script for your users that will identify them transparently as they log on to a Windows domain. See *Creating and Running the Script for Logon Agent*, page 196 for instructions.
- ◆ If you have Citrix users and non-Citrix users in your network, the same Websense components, except for Network Agent, can be used for both sets of users. A separate installation of Network Agent is needed for the Citrix users. See *Chapter 5 of the Installation Guide for Integrated Citrix® Servers* for configuration instructions. .
- ◆ If Network Agent was installed on a machine with multiple network interface cards (NICs), you can configure Network Agent to use more than one NIC. See *Configuring Network Agent to use Multiple NICs*, page 204.
- ◆ If Network Agent was installed, use the Traffic Visibility Tool to test whether Network Agent can see the user internet traffic that you want it to monitor. See *Testing Visibility of Internet Traffic to Network Agent*, page 204.

- ◆ If you were unable to grant User Service or DC Agent administrator privileges during installation, do so now to ensure that they will function correctly. See [Configure Domain Administrator Privileges](#), page 207.
- ◆ If you installed Websense Web Security Suite, activate your subscription to the Websense Web Protection Services™: SiteWatcher™, BrandWatcher™, and ThreatWatcher™. See [Activating the Websense Web Protection Services™](#), page 208 for instructions.
- ◆ If the optional Remote Filtering components were installed, the firewalls in your network must be configured to allow correct filtering of remote users. See [Firewall Configuration for Remote Filtering](#), page 209 for instructions.
- ◆ If you are using the optional Remote Filtering feature, you can configure how internet access requests from remote users are handled when the Remote Filtering Service is unavailable. See [Blocking remote users' internet access when Remote Filtering is unavailable](#), page 210 for instructions.
- ◆ If you are using the optional Remote Filtering feature, you can configure the size of the Remote Filtering Client's log file. See [Configuring the Remote Filtering Client Log](#), page 212 for instructions.

For additional Websense configuration information, see the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

---

## Subscription Key and Master Database Download

---

The Websense Master Database is the basis for filtering, and is updated daily by default. It is downloaded from a remote database server so that your version is the most current.

For the database download to occur, the machine running the Websense Filtering Service must have internet access to the download servers at the following URLs:

- ◆ download.websense.com
- ◆ ddsdom.websense.com
- ◆ ddsint.websense.com
- ◆ portal.websense.com
- ◆ my.websense.com

Make sure that these addresses are permitted by all firewalls, proxy servers, routers, or host files that control the URLs that the Filtering Service can access.

If you did not enter a subscription key to download the Master Database during installation, follow the instructions below to enter your key and download the Master Database now.

**Note**

If you have just upgraded your Websense software, your subscription key was retained by the installer and these steps are not necessary.

To download the Master Database:

1. Launch Websense Manager on any machine where it is installed.
  - **Windows 2000 Server:** Select **Start > Programs > Websense > Websense Manager**, or double-click the Websense Manager icon on the desktop.
  - **Windows Server 2003:** Select **Start > All Programs > Websense > Websense Manager**, or double-click the Websense Manager icon on the desktop.
  - **Solaris or Linux:** Go to the `/Manager` subdirectory in the Websense installation directory (by default, `opt/Websense/Manager`) and enter:

```
./start_manager
```
2. For a first-time installation, if Policy Server was not installed with Websense Manager, the **Add Policy Server** dialog box appears the first time you open Websense Manager.
  - a. Enter the IP address or machine name of the machine on which you installed the Policy Server, and the configuration port established during installation (default is 55806).
  - b. Click **OK**. The Policy Server machine's IP address or machine name appears beside a server icon in the Manager's navigation pane.
3. Double-click the icon of the Policy Server in the navigation pane.

For a first-time installation, the **Set Websense Password** dialog box appears.

4. Set a password (between 4 and 25 characters) for the Policy Server.



### Note

Retain this password. It must be entered when you connect to this Policy Server from this or any other Websense Manager, and when you log on to the Reporting Tools web interface.

5. Click **OK**.
  - If you have not yet entered your subscription or evaluation key, the **Settings** dialog box appears with the **Database Download** pane displayed.
  - If you entered your key during installation, navigate to the database download settings pane by selecting **Server > Settings > Database Download**.

The screenshot shows the 'Settings' dialog box with the 'Database Download' pane selected in the left-hand tree view. The 'Database Download' section includes the following fields and options:

- Download Days:** A row of checkboxes for days of the week: S (checked), M (checked), Tu (checked), W (checked), Th (checked), F (checked), Sa (checked).
- Download Between:** Two time selection boxes. The first is set to '21:00' and the second to '06:00', with 'and' between them.
- Subscription Key:** An empty text input field.
- Key Expires:** A text input field.
- Subscribed network users:** 0
- Subscribed remote users:** 0

Below the Database Download section are three other sections:

- Real-Time Security Updates:** Includes a checkbox for 'Enable real-time security updates' (unchecked) and a note: 'Real-time security updates occur when new threats are identified. Standard daily downloads at the specified times include all other updates.'
- Proxy Server:** Includes a checkbox for 'Use Proxy Server' (unchecked), a 'Server:' text input field, and a 'Port:' text input field with '8080' entered.
- Authentication:** Includes a checkbox for 'Use Authentication' (unchecked), a 'User name:' text input field, and a 'Password:' text input field.

At the bottom of the dialog box are three buttons: 'OK', 'Cancel', and 'Help'.

Database Download Settings

6. Enter your alphanumeric key in the **Subscription Key** field.



The **Subscribed network users** and **Subscribed remote users** fields show a value of **0** until the database is successfully downloaded.

7. If your network requires that browsers use an upstream proxy server to reach the internet, the same proxy settings used by the browser must be used for downloading the Websense Master Database. Establish the proxy settings for the database download as follows:

- a. Check **Use Proxy Server**.
- b. Identify the upstream proxy server or firewall by entering the machine's IP address or machine name in the **Server** field.

Supported machine name formats are as follows:

- **Windows:** 7-bit ASCII and UTF-8 characters. The DNS server must be able to recognize UTF-8 characters and resolve the name into an IP address. Do NOT use a machine name that has extended ASCII or double-byte characters.
- **Solaris or Linux:** 7-bit ASCII only.



#### **Note**

If Websense software is installed on a proxy server machine in your network, *do not* enter that IP address in your proxy settings. Use **localhost** instead.

---

- c. Enter the **Port** of the upstream proxy server or firewall (default is 8080).
8. If your network requires authentication to an upstream proxy server or firewall to reach the internet and download the Websense Master Database, perform the following procedure:
    - a. Check **Use Authentication**.
    - b. Be sure to configure the upstream proxy server or firewall to accept clear text or basic authentication (to allow download of the Master Database).
    - c. Enter the **User name** required by the upstream proxy server or firewall to download the Master Database.
    - d. Enter the **Password** required by the upstream proxy server or firewall.
  9. Click **OK** to save your changes.

The Websense Filtering Service automatically contacts the Websense database server and begins downloading the Master Database. The status of the download is displayed in the **Database Download** dialog box. When the download has completed, the **Last Download Result** field displays **Successful**.

10. Click **Close** in the **Database Download** dialog box when the download is complete.



**Note**

After downloading the Master Database or updates to the Master Database, and when the Filtering Service is started, CPU usage can be 90% or more while the database is loaded into local memory.

---

To download the Websense Master Database manually at any time, choose **Server > Database Download** in Websense Manager.

## Identifying the Filtering Service for the Block Page URL

---

If the Filtering Service is installed on a multihomed machine (with two or more network interface cards), you must identify the Filtering Service by its IP address in your network so that Websense block messages can be sent to users.

When Websense software blocks an internet request, the user's browser is redirected by default to a block message page hosted by the Filtering Service. The block page URL typically takes the form:

**http://<WebsenseServerIPAddress>:<MessagePort>/cgi-bin/  
blockpage.cgi?ws-session=#####**

If the Filtering Service machine name, rather than the IP address, is contained in the block page URL, users could see a blank page instead of the block message that tells them why the site is blocked.

Identify the Filtering Service by IP address to ensure that block pages display correctly on users' workstations:

- ◆ If you have an internal DNS server, associate the machine name of the Filtering Service machine with its correct (typically internal) IP address by entering the IP address as a resource record in your DNS server. See your DNS server documentation for instructions.

- ◆ If you do not have internal DNS, add an entry to the `eimserver.ini` file by following these instructions:
  1. On the Filtering Service machine, go to the `\bin` folder in the Websense installation directory (by default, `Websense\bin`).
  2. Make a backup copy of the `eimserver.ini` file and store it in another folder.
  3. Open the original `eimserver.ini` file in a text editor.
  4. In the `[WebsenseServer]` area, enter the following command on a blank line:

```
BlockMsgServerName=<IP address>
```

where `<IP address>` is the correct (typically internal) IP address of the machine running Filtering Service.



### Important

*Do not* use the loopback address 127.0.0.1.

---

5. Save the file.
6. Stop and then restart the Filtering Service (see [Stopping or Starting Websense Services](#), page 185).

## Displaying Protocol Block Messages

---

Websense software will filter protocol requests normally whether or not protocol block messages are configured to display on user workstations.

Protocol block messages cannot be displayed on the following workstation operating systems:

- ◆ Solaris
- ◆ Linux
- ◆ Macintosh



**Note**

Windows XP Service Pack 2 only displays protocol block messages under the following conditions:

- ◆ The firewall function must be either be disabled or modified not to block the messages.
- ◆ The Windows Messenger service must be started.

---

For users to view protocol block messages in Windows NT, Windows 2000, and Windows Server 2003:

- ◆ Make sure that the User Service has administrator privileges. For instructions, see [Configure Domain Administrator Privileges, page 207](#).
- ◆ Make sure the Messenger Service is enabled on *each* client workstation that is being filtered. If you have activated Websense protocol management, check the Windows **Services** dialog box to see if the Messenger Service is running. If your company policy requires the Messenger Service to be disabled, you should advise your users that certain protocols will be blocked without notification.

To view protocol block messages on a Windows 98 machine, you must start `winpopup.exe`, found in the Windows directory of your local drive. You can start this application from a command prompt or configure it to start automatically by copying it into the Startup folder. For instructions, see your operating system documentation.

## Creating and Running the Script for Logon Agent

---

If you have installed Websense Logon Agent, you must create a logon script for your users that will identify them transparently as they log on to a Windows domain. Identification is accomplished by the Websense `LogonApp.exe` application, which provides a user name and IP address to the Logon Agent each time a Windows client machine connects to an Active Directory or a Windows NTLM directory service.

### Prerequisites for Running the Logon Script

Make the following network preparations so that the Websense logon script can execute properly on users' Windows workstations:

- ◆ Be sure that all workstations can connect to the shared drive on the domain controller where the logon script and `LogonApp.exe` will be placed. To determine if a workstation has access to the domain controller, run the following command from a Windows command prompt:

```
net view /domain:<domain name>
```
- ◆ NetBIOS for TCP/IP must be enabled. In Windows 98, TCP/IP NetBIOS is enabled by default.
- ◆ The TCP/IP NetBIOS Helper Service must be running on each client machine that will be identified by Logon Agent. This service runs on Windows 2000, Windows XP, Windows Server 2003, and Windows NT®.

## File Location

All relevant files are located in the `websense\bin` folder on the Logon Agent machine:

- ◆ `LogonApp.exe`: the Websense executable that communicates user information to the Logon Agent.
- ◆ `Logon.bat`: batch file containing sample logon and logout scripts.
- ◆ `LogonApp_ReadMe.txt`: a summary of the procedures for creating and running the Websense logon script and optional logout script.

## Deployment Tasks

To deploy `LogonApp.exe` with a logon script, perform the following tasks:

**Task 1: Prepare the logon script:** Edit the parameters in the sample script file (`Logon.bat`) to suit your needs. This file contains two sample scripts: a logon script and a logout script. Active Directory can use both types of scripts. If you plan to use both types, you will need two separate `.bat` files with different names.

**Task 2: Configure the script to run:** You can run your logon script from Active Directory or Windows NTLM directory services using group policies. This requires you to move the Websense executable and logon batch file to a shared drive on the domain controller that is visible to all user workstations. If you use Active Directory, you may create and deploy an optional logout batch file on the shared drive.

## Preparing the Logon Script

A batch file, called `Logon.bat`, is installed with Logon Agent in the `Websense\bin` folder. This file contains some instructions for using the scripting parameters, and two sample scripts: a logon script that runs `LogonApp.exe`, and a logout script for Active Directory that removes user information from the Websense user map when the user logs out.

### Script Parameters

Using the samples provided, construct a script for your users that employs the parameters in the following table. The required portion of the script is:

```
LogonApp.exe http://<server>:<port>
```

This command runs `LogonApp.exe` in *persistent* mode (the default), which sends user information to the Logon Agent at predefined intervals.

**Note**

You can edit the sample, or create a new batch file containing a single command.

---

Parameter	Description
<code>&lt;server&gt;</code>	IP address or name of the machine running the Websense Logon Agent. This must match the machine address or name entered when you configured Logon Agent in Websense Manager.
<code>&lt;port&gt;</code>	The port number used by Logon Agent. Enter 15880 if you accepted the default port number when you configured Logon Agent in Websense Manager.

Parameter	Description
/NOPERSIST	<p>Causes LogonApp.exe to send user information to the Logon Agent at logon only. The user name and IP address are communicated to the server at logon and remain in the Websense user map until the user's data is automatically cleared at a predefined time interval. The default interval is 24 hours.</p> <p>If the NOPERSIST parameter is not present, LogonApp.exe operates in the <i>persistent</i> mode. In persistent mode, LogonApp.exe resides in memory on the domain server and updates the Logon Agent with the user names and IP addresses at predefined intervals. The default interval is 15 minutes.</p> <p>For information about configuring Logon Agent via Websense Manager, see the User Identification chapter in the <i>Administrator's Guide</i> for Websense Enterprise/Web Security Suite.</p>
/COPY	<p>Copies the LogonApp.exe application to the users' machines, where it is run by the logon script from local memory. This optional parameter can be helpful if you experience any hangs with your logon script. The application is copied into the %USERPROFILE%\Local Settings\Temp folder. COPY can be used only in the <i>persistent</i> mode.</p>
/VERBOSE	<p>Debugging parameter that must be used only at the direction of Technical Support.</p>
/LOGOUT	<p>(Used only in an optional logout script) Removes the user's logon information from the Websense user map when the user logs off. If you use Active Directory, you can use this parameter to clear the logon information from the user map before the interval defined in Logon Agent has elapsed. Use this optional parameter in a logout script in a different batch file than the one containing the logon script. See the example scripts below.</p>

## Websense User Map and the Persistent Mode

User identification provided at logon by LogonApp.exe is stored in the Websense user map. This information is updated periodically if LogonApp.exe is run in persistent mode. The update time interval for the persistent mode and the interval at which the user map is automatically cleared of logon information are configured in the **Logon Agent** tab of the **Settings** dialog box in Websense Manager. In Active Directory, if you decide to clear the logon information from the Websense user map before the interval defined in the Manager, you can create an accompanying logout script. You cannot configure a logout script with Windows NTLM.

In the non-persistent mode, information in the user map is created at logon and is not updated. The use of the non-persistent mode creates less traffic between the Websense software and the workstations in your network than does the persistent mode.

For detailed information about configuring Logon Agent in Websense Manager, see the User Identification chapter in the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

## Examples

The following are examples of commands for a logon script and the companion logout script that might be run in Active Directory. The two scripts must be run from separate batch files.

- ◆ **Logon Script:** In this example, the edited `Logon.bat` file contains this single command:

```
LogonApp.exe http://10.2.2.95:15880 /NOPERSIST
```

The sample script above sends user information to the Logon Agent at logon only. The information is not updated during the user's session (`NOPERSIST`). The information is sent to port 15880 on the server machine identified by IP address 10.2.2.95.

With Active Directory you have the option to clear the logon information for each user as soon as the user logs out. (This alternative is not available with Windows NTLM.) To accomplish this, you create a companion logout script in a different batch file.

- ◆ **Logout Script:** Continuing the example, copy the logon batch file and rename it `Logout.bat`. Then edit the script in `Logout.bat` as shown here:

```
LogonApp.exe http://10.2.2.95:15880 /NOPERSIST /LOGOUT
```



## Configuring the Logon Script to Run

You can configure your logon script to run with a group policy on Active Directory or on a Windows NTLM directory service.



### Note

The following procedures are specific to Microsoft operating systems and are provided here as a courtesy. Websense, Inc., cannot be responsible for changes to these procedures or to the operating systems that employ them. For more information, see the links provided.

### Active Directory

If your network uses Windows 98 client machines, go to the Microsoft website for assistance.

To configure a logon script (and optional logoff script) using Active Directory:

1. Make sure your environment meets the conditions described in [Prerequisites for Running the Logon Script, page 196](#).
2. On the Active Directory machine, go to the Windows **Control Panel** and select **Administrative Tools > Active Directory Users and Computers**.
3. Right-click the domain and select **Properties**.  
The domain **Properties** dialog box appears.
4. Select the **Group Policy** tab.
5. Click **New** and create a policy called **Websense Logon Script**.
6. Double-click your new policy or click **Edit** to edit the policy.  
The **Group Policy Object Editor** dialog box appears.
7. In the tree structure displayed, expand **User Configuration**.
8. Expand the **Windows Settings** structure.
9. Select **Scripts (Logon/Logoff)**.
10. In the right pane, double-click **Logon**.
11. In the **Logon Properties** dialog box displayed, click **Show Files** to open the logon script folder for this policy.  
The folder opens in a Windows Explorer window.

12. Copy two files into this folder: your edited logon batch file (`Logon.bat`) and the application `LogonApp.exe`.
13. Close the Explorer window and click **Add** in the **Logon Properties** dialog box.

The **Add a Script** dialog box appears.
14. Enter the file name of the logon batch file (`Logon.bat`) in the **Script Name** field or browse for the file.
15. Leave the **Script Parameters** field empty.
16. Click **OK** twice to accept the changes.
17. (Optional.) If you have prepared a logout script, repeat [Step 7](#) through [Step 16](#). Choose **Logoff** at [Step 10](#), and use your logout batch file whenever you are prompted to copy or name the batch file.
18. Close the **Group Policy Object Editor** dialog box.
19. Click **OK** in the domain **Properties** dialog box to apply the script.
20. Repeat this procedure on each domain controller in your network as needed.



#### Note

You can determine if your script is running as intended by configuring your Websense software for manual authentication. If transparent authentication with Logon Agent fails for any reason, users will be prompted for a user name and password. Advise your users to notify you if this occurs. To enable manual authentication, follow the instructions in the User Identification chapter of the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

---

For additional information about deploying logon scripts to users and groups in Active Directory, please see:

<http://technet2.microsoft.com/WindowsServer/f/?en/library/84b5457b-1641-4707-a1f4->

## Windows NTLM

To configure the Websense logon script in Windows NTLM:

1. Make sure your environment meets the conditions described in [Prerequisites for Running the Logon Script, page 196](#).
2. Copy the `Logon.bat` and `LogonApp.exe` files from the `websense\bin` folder on the Logon Agent machine to the netlogon share directory on the domain controller machine.

```
C:\WINNT\system32\Repl\Import\Scripts
```

Depending on your configuration, you may need to copy these files to other domain controllers in the network to run the script for all your users.

3. In the **Control Panel** of the domain controller, select **Administrative Tools > User Manager for Domains**.
4. Select the users for whom the script must be run and double-click to edit the user properties.

The **User Properties** dialog box appears.

5. Click **Profile**.

The **User Environment Profile** dialog box appears.

6. Enter the path to the logon batch file in the **User Profile Path** field (from [Step 2](#)).
7. Enter the name of the logon batch file (`Logon.bat`) in the **Logon Script Name** field.
8. Click **OK**.
9. Repeat this procedure on each domain controller in your network as needed.



### Note

You can determine if your script is running as intended by configuring your Websense software for manual authentication. If transparent authentication with Logon Agent fails for any reason, users will be prompted for a user name and password. Advise your users to notify you if this occurs. To enable manual authentication, follow the instructions in the User Identification chapter in the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

## Configuring Network Agent to use Multiple NICs

---

Each Network Agent instance must use at least one designated NIC. However, Network Agent is capable of using multiple NICs. If you installed Network Agent on a machine with multiple NICs, you can configure it to use different NICs for different purposes. For example, you can configure Network Agent to use one NIC for monitoring traffic, and another to send blocking information to Filtering Service.

To configure Network Agent to use additional NICs, follow the instructions in the Network Agent chapter in the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

## Testing Visibility of Internet Traffic to Network Agent

---

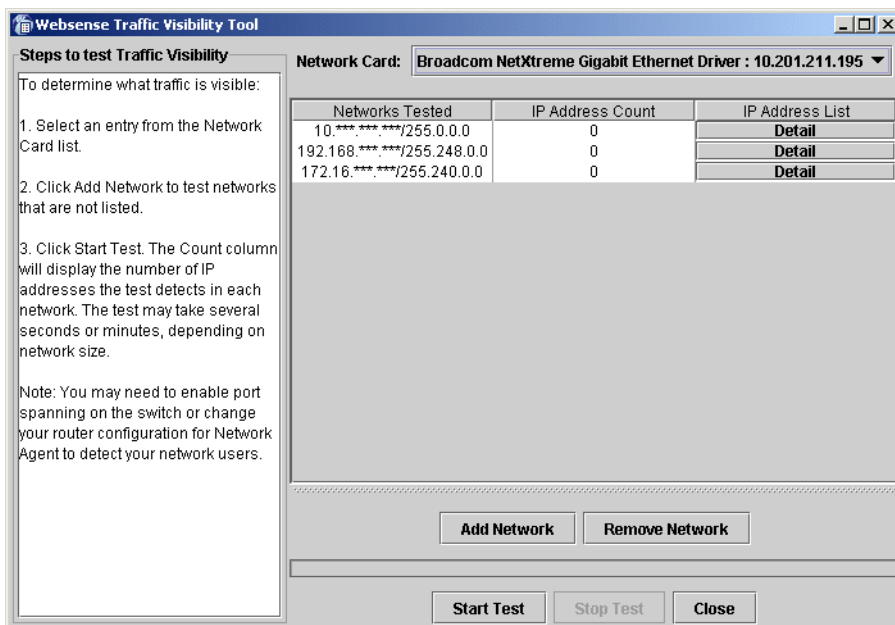
If you installed Network Agent and have any doubt about its ability to monitor internet requests from the desired network and to see the replies, you can conduct a traffic visibility test on the Network Agent machine using the Websense Traffic Visibility Tool.

### Running the Websense Traffic Visibility Tool

Run the Websense Traffic Visibility Tool on the Network Agent machine to test internet traffic visibility. The NIC that Network Agent is configured to use must be able to monitor 2-way employee internet traffic for Network Agent to function properly.

1. To start the tool:
  - **Windows:** From the **Start** menu, choose **Programs** (or **All Programs**) > **Websense** > **Utilities** > **Traffic Visibility Tool**.
  - **Linux or Solaris:** Run `./TrafficVisibility.sh` from the Websense installation directory (`/opt/Websense`).  
To start a GUI version, run `./TrafficVisibility.sh -g`

The Websense Traffic Visibility Tool appears.



Traffic Visibility Tool

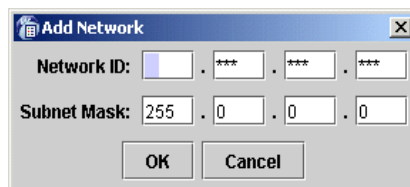
Field	Description
Network Card	Name of the network interface card (NIC) to test. Active cards on the installation machine appear in this list. Cards without an IP address will not appear in this list.
Networks Tested	Displays the netmasks that are being tested. You may use the defaults provided or add your own. These netmasks can reside in different network segments depending upon the IP address ranges to be filtered.
IP Address Count	Number of IP addresses for which traffic is detected during the test of a network.
IP Address List Detail	Lists all the IP addresses in the network from which internet traffic is being detected.

2. From the **Network Card** drop-down list, select the network interface card (NIC) that the Network Agent is configured to use.

A default list of networks (netmasks) to test appears. You may use the defaults provided or add your own. These netmasks can reside in different network segments depending upon the IP address ranges to be filtered.

3. If the network you want to test with the NIC does not appear in the default list, click **Add Network**.

The **Add Network** dialog box appears.



- a. Enter a new netmask value in the **Network ID** field.

The subnet mask defaults to 255.0.0.0 and changes appropriately as the netmask is defined.

- b. Click **OK** to return to the Websense Traffic Visibility Tool dialog box. Your new network appears in the list.

4. Select **Remove Network** to delete a network from the list.
5. Click **Start Test** to begin testing all the networks in the list.

The counter in the **IP Address Count** column should begin recording internet traffic immediately from the networks listed. The counter increments each time the NIC detects an individual IP address from the target network in a passing packet. The activity bar at the bottom of the dialog box indicates that a test is in progress.

If the count for a network remains at zero or is very low, the selected NIC cannot see the traffic it is supposed to monitor.

6. If the Network Agent NIC is unable to see the desired traffic, perform one or both of the following tasks:
  - If the installation machine has multiple NICs, select a different card to test. If this card can see the desired traffic, configure Network Agent to use this card. For instructions, see the Network Agent chapter in the *Administrator's Guide* for Websense Enterprise/Web Security Suite.
  - Resolve network configuration issues to make sure that the NIC can see the desired traffic. This might involve connecting to a different router or configuring for port spanning in a switched environment. See [Chapter 2: Network Configuration](#) for deployment information. Make the necessary changes and retest the NIC.

7. Click **Stop Test** when you are finished testing.
8. Click **Close** to exit the Traffic Visibility Tool.

The Network Agent NIC must be able to monitor all targeted internet traffic. If Network Agent cannot see the necessary traffic, you must either reposition the machine in the network, or select another machine on which to install the Network Agent.

---

## Configure Domain Administrator Privileges

---

User Service and DC Agent must have administrator privileges on the network to retrieve user logon information from the domain controller. If you were not able to grant these privileges during installation, you can do so now.

### User Service and DC Agent on Windows

If you were unable to grant User Service or DC Agent domain administrator privileges during installation on a Windows machine, you can edit the properties of these services now so that they can access directory service information. This procedure may vary slightly, depending upon the version of Windows you are using.

1. From the Control Panel on the installation machine, select **Administrative Tools > Services**.
2. In the **Services** dialog box, double-click **Websense User Service**.
3. Select the **Log On** tab in the **Properties** dialog box.
4. Select **This account** and enter a valid domain/user name and password for an account with **domain** administrator privileges in your network.
5. Click **OK**.
6. If DC Agent was installed, repeat the process for the **Websense DC Agent** service.

### DC Agent on Linux

If you installed DC Agent on Linux, but were unable to grant it administrator privileges on the domain controller during installation, follow these steps.

1. In Websense Manager, select **Server > Settings**, and then select **Directory Service** in the left-hand pane.

2. Select **Windows NT Directory / Active Directory (Mixed Mode)**. (Make this selection even if you are not using Mixed Mode.)
3. Enter domain administrator credentials in the fields on the screen.
4. Click **OK**.

## Activating the Websense Web Protection Services™

---

The Websense® Web Protection Services™—SiteWatcher™, BrandWatcher™, and ThreatWatcher™—protect your organization’s websites, brands, and web servers. These services are included if you purchased a Web Security Suite subscription, but they must be activated.

To turn on ThreatWatcher, SiteWatcher, and BrandWatcher:

1. Go to [www.my.websense.com](http://www.my.websense.com), log in, and enter your Web Security Suite subscription key.
2. On your My Websense main page, go to the Websense Security Labs box.
3. Click the links beside each of the services in turn, and follow the onscreen instructions.

The following sections provide a brief description of each of the Web Protection Services. More information is available at [www.websense.com](http://www.websense.com).

### SiteWatcher™

SiteWatcher alerts you when your organization’s websites have been infected with malicious mobile code. SiteWatcher allows you to take immediate action to prevent its spread to customers, prospects, and partners who might visit the website.

### BrandWatcher™

BrandWatcher alerts you when your organization’s websites or brands have been targeted in phishing or malicious keylogging code attacks. BrandWatcher provides you with internet security intelligence, attack details, and other security-related information so that you can take action, including notifying your customers and minimizing any public relations impact.



## ThreatWatcher™

ThreatWatcher provides you with a *hacker's-eye* view of your organization's web server, regularly scanning for known vulnerabilities and potential threats, and reporting on risk levels and recommended actions through a web-based portal. ThreatWatcher helps you prevent malicious attacks on your web servers before they happen.

## Firewall Configuration for Remote Filtering

---

Remote Filtering is an optional Websense service that allows you to filter user workstations located outside your organization's network firewall. If you installed the Remote Filtering components, some firewall configuration is necessary to enable web filtering on remote workstations. Firewalls must be configured to allow the Remote Filtering Server to communicate with the remote workstations and with the Filtering Service.

### Enabling communication between Remote Filtering Server and Remote User Workstations

The external network firewall and any additional firewalls located between the Remote Filtering Server machine and the remote workstations should be configured as follows:

- ◆ Open the Remote Filtering Server's **External Communication Port** on these firewalls to accept connections from Remote Filtering Clients on workstations located outside the network firewall. By default, this is port 80, unless it was changed during installation of the Remote Filtering Server.
- ◆ Block connections to the Remote Filtering Server's **Internal Communication Port** from workstations located outside the network firewall. By default, this is port 8800, unless it was changed during installation of the Remote Filtering Server.

See the documentation for your firewall product if you need information about how to accomplish these firewall configuration tasks.

## Enabling communication between Remote Filtering Server and Filtering Service

If there is a firewall between the Remote Filtering Server machine and the Filtering Service machine, configure it as follows:

- ◆ Open the Filtering Service's **Filter port** (by default, 15868) on this firewall to accept connections from the Remote Filtering Server.
- ◆ Open the Filtering Service's **Block Page port** (by default, 15871) on this firewall to allow Filtering Service to serve block pages to remote users.

See the documentation for your firewall product if you need information about how to accomplish these firewall configuration tasks.

## Blocking remote users' internet access when Remote Filtering is unavailable

---

If you are using the optional Websense Remote Filtering feature, you can configure it to block remote users' internet access when they are unable to connect with the Remote Filtering Server. You can also configure the length of time that the Remote Filtering Client on a remote user's machine will attempt to connect with a Remote Filtering Server before failing closed and blocking access to all websites.

This behavior is controlled by the following two parameters in the `securewisproxy.ini` file on the Remote Filtering Server machine:

- ◆ **FailClose:** The `FailClose` parameter specifies whether a Remote Filtering Client fails open or closed when connectivity with the Remote Filtering Server is lost.
  - When set to `false`, the Filtering Client fails open and all HTTP traffic is allowed. The default value is `false`.
  - When set to `true`, the Filtering Client fails closed and all HTTP traffic is blocked.
- ◆ **FailCloseTimeout:** The `FailCloseTimeout` parameter applies only when Remote Filtering clients are set to fail closed (`FailClose=true`). `FailCloseTimeout` specifies the amount of time, in minutes, that the Remote Filtering Client tries to connect with the Remote Filtering Server before failing closed and blocking all HTTP traffic. During this time, all

HTTP traffic is permitted. The default value is 15, but can be set to any integer from 0 to 60. A value of 0 disables the timeout. If any other value is entered, the default of 15 minutes is enforced.

To set these parameters so that remote users' internet access is blocked when they are unable to establish a connection with the Remote Filtering Server:

1. On the Remote Filtering Server machine, locate the `securewispproxy.ini` file in the `bin` subdirectory in the Websense installation directory. The default location of this file is:
  - Windows: `\Program Files\Websense\bin`
  - Linux and Solaris: `/opt/Websense/bin`
2. Open the `securewispproxy.ini` file in a text editor.
3. Change the value of the `FailClose` parameter to `true`.
4. If you leave the `FailCloseTimeout` set to its default value of 15, the Remote Filtering Client tries to connect with the Remote Filtering Server for 15 minutes before failing closed and blocking all HTTP traffic.
  - To change the length of time, in minutes, that the Remote Filtering Client tries to connect, change the value of `FailCloseTimeout` to an integer from 1 to 60.
  - To disable the timeout, change the value of `FailCloseTimeout` to 0. The Remote Filtering Client keeps trying to establish a connection.
5. Save your changes.
6. Restart the Remote Filtering Server.

For instructions, see *Stopping or Starting Websense Services*, page 185.

The new settings are applied to all Remote Filtering Clients that connect with the Remote Filtering Server.



---

**Note**

If you are using Websense Client Policy Manager (CPM) in your network, Remote Filtering parameters are configured in the Desktop tab of Websense Manager. If the CPM Server is present, values set for the `FailClose` and `FailCloseTimeout` parameters in the `securewisproxy.ini` file are ignored.

For information about configuring Remote Filtering features when you are using CPM, see your Websense Client Policy Manager documentation.

---

## Configuring the Remote Filtering Client Log

---

If you are using the optional Websense Remote Filtering feature, each Remote Filtering Client installed on a user workstation maintains a local log file.

The Remote Filtering Client logs each time the Client:

- is activated after the machine leaves the corporate network
- is deactivated after the machine enters the corporate network
- is restarted
- fails open (allows access to all websites when connectivity with Remote Filtering Server is lost)
- fails closed (blocks access to all websites when connectivity with Remote Filtering Server is lost)
- receives a policy update

The maximum size of this local log file can be changed by editing the `LocalLogSize` parameter in the `securewisproxy.ini` file on the Remote Filtering Server machine.

The `LocalLogSize` parameter defines the maximum size, in MB, of the log file. Once the maximum file size is reached, the log file name is time stamped with the current date and time and saved. A maximum of two log files are maintained; the oldest log is deleted when a third log is started. The default

value of `LocalLogSize` is 1, but it can be set to any integer from 0 to 10. To disable the log, enter a value of 0.

To change the maximum size of the Remote Filtering Client's local log file:

1. On the Remote Filtering Server machine, locate the `securewispproxy.ini` file in the `bin` subdirectory in the Websense installation directory. The default location of this file is:
  - Windows: `\Program Files\Websense\bin`
  - Linux and Solaris: `/opt/Websense/bin`
2. Open the `securewispproxy.ini` file in a text editor.
3. Change the value of the `LocalLogSize` parameter to any integer from 0 to 10.

This integer defines the maximum size of the log in MB. A value of 0 disables the log.
4. Save your changes.
5. Restart the Remote Filtering Server. For instructions, see [Stopping or Starting Websense Services](#), page 185.

The new maximum log size setting is applied to all Remote Filtering Clients that connect with the Remote Filtering Server.

**Note**

If you are using Websense Client Policy Manager (CPM) in your network, Remote Filtering parameters are configured in the Desktop tab of Websense Manager. If the CPM Server is present, values set for the `LocalLogSize` parameter in the `securewispproxy.ini` file are ignored.

For information about configuring Remote Filtering features when you are using CPM, see your Websense Client Policy Manager documentation.

---



# Using FireWall-1 with Websense Software

Check Point FireWall-1 provides network security and a framework for content filtering. Websense Enterprise/Web Security Suite communicates with FireWall-1 via the URL Filtering Protocol (UFP). Technically, Websense filtering software is implemented as a UFP Server. Websense software communicates with FireWall-1 over TCP (Transmission Control Protocol) sockets. By default, the Websense software listens for FireWall-1 messages on port 18182.

To begin filtering:

- ◆ Client machines must point to FireWall-1 as their default gateway in order to be filtered. Typical networks implement this for security reasons unrelated to filtering.
- ◆ FireWall-1 must be configured so that all HTTP requests to be filtered (and FTP requests issued by a browser that proxies to FireWall-1) are analyzed by a FireWall-1 rule that uses the URI Specifications for HTTP.



## Note

If Websense Enterprise/Web Security Suite must download the Master Database through a proxy server or firewall that requires authentication for any HTTP traffic, the proxy server or firewall must be configured to accept clear text or basic authentication.

---

When Websense Enterprise/Web Security Suite is integrated with FireWall-1, you define policies within Websense Manager (the configuration interface for Websense filtering software). These policies identify which of the Websense categories are blocked or not blocked during different times and days. Within FireWall-1, you typically define a rule that directs the firewall to reject

requests for sites in the block, limit by quota, or continue Websense categories. If a user selects an option to view a site on a block page, Websense software tells FireWall-1 to permit the site.

Policies can be applied to individual workstations, as defined by IP address, or to a range of IP addresses defined as a Websense network. If you implement the Websense transparent identification features, or activate manual authentication within the Websense software, you also can apply policies to individual users, groups, domains/organizational units (called directory objects) defined within your organization's directory service. In Websense software, directory objects, workstations, and networks are known collectively as *clients*.

When FireWall-1 receives an internet request for an HTTP site (or an FTP site requested by a browser that uses the firewall as a proxy), it queries the Websense software to determine whether the site should be blocked or not. Based on the source of the request and the time of day, the Websense filtering software evaluates the applicable policies, determining whether the requested URL is in a category whose filtering setting is block, permit, limit by quota, or continue, or is not in the Master Database. (For a description of this evaluation, see the *Administrator's Guide* for Websense Enterprise/Web Security Suite.) The Websense software sends an appropriate response to FireWall-1, which then accepts or rejects the request according to its Rule Base.

When a request is accepted, FireWall-1 returns the site to the client. If the request is rejected, the Websense software displays a block message that tells why the site is blocked. If the associated category is limited by quota, the Websense block message includes options for using quota time to view the site. If the associated category is continue, the Websense block message includes an option to continue and view the site for business purposes.



## Distributed FireWall-1 Environments

---

In environments where the FireWall-1 Management Server is separated from the FireWall-1 Module, you must modify your FireWall-1 policy to allow the Management Server to communicate with the Websense Filtering Service during setup for the purpose of loading the dictionary. All other communication will be between the Websense Filtering Service and the FireWall-1 Module.



### Note

Websense, Inc., and Check Point recommend installing Websense components on a different machine than the machine on which FireWall-1 is installed. If, for any reason, Websense software and FireWall-1 must be installed on the same machine, see the Websense Knowledge Base at [www.websense.com/docs/](http://www.websense.com/docs/) for configuration instructions.

---

## Client Workstations and FireWall-1

---

FireWall-1 processes HTTP requests transparently; therefore, no internet browser changes are required on client workstations. You may, however, choose to have clients proxy to the firewall to enable user authentication within FireWall-1 or to enable filtering of FTP requests from a browser. See the FireWall-1 documentation for further information about setting up FireWall-1 to send FTP requests through the HTTP Security Server.

If clients will use the firewall as a proxy, client workstations must run a web browser that supports proxy-based connections, such as version 4.x or higher of Netscape Navigator or Internet Explorer.

## Communicating with Websense Software

---

Depending on which version of FireWall-1 is running, Websense software may communicate with the firewall through a secure connection or a clear connection. A secure connection requires that communication between FireWall-1 and the Websense UFP Server is authenticated before any data is

exchanged. A clear connection allows the Websense software and FireWall-1 to transfer data without restrictions.

The following list identifies the options available for each supported FireWall-1 version:

- ◆ **FireWall-1 NG Feature Pack 1 or later:** clear connection is the default, but a Secure Internal Communication (SIC) trust connection can be configured within both FireWall-1 and the Websense software.
- ◆ **FireWall-1 NG with Application Intelligence (AI):** clear connection is the default. An authenticated connection can be established, but is not recommended because of performance issues. In addition, a clear connection is required to use the Enhanced UFP Performance feature described in the following section.
- ◆ **FireWall-1 NGX:** clear connection is the default. An authenticated connection can be established, but is not recommended because of performance issues. In addition, a clear connection is required to use the Enhanced UFP Performance feature described in the following section.

See [Chapter 7: Configuring FireWall-1 NG, NG with AI, and NGX](#) for the appropriate procedures to establish secure or clear communication with the Websense filtering software.

## Enhanced UFP Performance

---

In FireWall-1 NG with Application Intelligence (AI) and FireWall-1 NGX, Check Point has improved the performance of the UFP Server with the Enhanced UFP Performance feature (QuickUFP). QuickUFP increases the amount of traffic that the Websense software and FireWall-1 can filter while reducing CPU load.

Configuring for Enhanced UFP Performance requires the proper settings in both the Websense software and FireWall-1. See [Enhanced UFP Performance, page 245](#) for detailed configuration procedures.



### Note

To use the Enhanced UFP Performance feature, the Websense software and FireWall-1 must be configured for clear communication.

---

## Caching

---

FireWall-1 offers the option to cache the IP address (not the URL or content) of certain sites, based on the Websense response. When FireWall-1 receives a request, it first checks the cache. If the site's IP address is found, FireWall-1 permits the site from the cache without contacting the Websense software.



### Note

The Websense software logs include only those internet requests submitted to the Websense software for filtering. When caching is enabled, requests handled from the cache cannot be logged by the Websense software, and are not included in reports generated by the Websense Reporting Tools. However, FireWall-1 logs may include this information.

---

## Strategy

Choosing the right caching option requires an understanding of which factors are most important in your environment. Many organizations activate different options for a period of time, and then evaluate which option best meets their needs.

Key factors that influence your caching choice include:

- ◆ **Performance:** the speed at which FireWall-1 can return the requested site to the user's browser. Caching stores the IP address of certain sites that Websense Enterprise permits. If FireWall-1 can approve the request from the cache, without submitting it to the Websense software, response time is faster. The caching option you select affects how many IP addresses can be cached.
- ◆ **Accuracy:** the number of sites that are blocked correctly. Lower accuracy means users can access sites that should be blocked because the associated IP address has been cached as permitted. Increased accuracy results in less of this "under blocking."
- ◆ **Flexibility:** the need to define different filtering strategies for different times and days, or for different clients (users, groups, domains/ organizational units, workstations, or networks). Increased flexibility

requires that fewer IP addresses be cached. Decreased flexibility means that more IP addresses can be cached.

Caching can increase performance, but it must be used carefully to prevent users from having access to sites that should be blocked. The caching options available depend on which version of FireWall-1 is running. Review the following information to determine which caching option is best for your environment.



### Important

Any time you modify your Websense filtering policies, be sure to clear the cache by installing the firewall policy, or by restarting the firewall, or by entering `fw tab -x -t ipufp_cache` at the firewall machine. Otherwise, the cache might permit sites that should be blocked by the revised policy.

---

## Options

FireWall-1 includes a **UFP caching control** area on the **Match** tab of the **URI Resource Properties** dialog box. This section summarizes the FireWall-1 caching options available in this area. To select a caching option, open the **UFP caching control** drop-down list.

See [Creating Resource Objects, page 228](#) for information about how to access the **Match** tab and make selections. Please read your FireWall-1 documentation for more complete information.

### No Caching (Recommended)

No caching offers the most versatile and accurate filtering, at the expense of a slight decrease in performance as compared to caching performance.

Choosing **No caching** allows you to take advantage of all the Websense features, including the ability to create and assign separate filtering policies to individual clients, keyword blocking, and custom URLs.

With the **No caching** option selected, FireWall-1 submits every HTTP request and certain FTP requests to the Websense filtering software. The Websense software compares each request to the policy assigned to the client making the request, and returns the appropriate response, which depends on the filtering option selected for the active category set in the policy.

## UFP Server Caching

UFP Server caching is not supported by the Websense UFP Server. If you select UFP Server caching, no caching will occur.

## One-Request Caching

One-request caching is called *VPN-1 Pro/Express (one-request) caching* in FireWall-1 NGX, and *VPN-1 and FireWall-1 (one-request) caching* in FireWall-1 NG and FireWall-1 NG with AI. One-request caching is appropriate for larger organizations with high internet volume, providing excellent performance and reasonable caching accuracy at the expense of flexibility.

With one request caching, FireWall-1 submits the requested URL to the Websense filtering software. If the Websense software permits the site, FireWall-1 caches the IP address. All subsequent requests for sites with the same IP address will be permitted from the cache, regardless of the requestor or the time of day.

This caching option can increase performance, but may lead to some under blocking, particularly with virtual hosts, which can host sites from multiple Websense categories at the same IP address. Additionally, once the Websense software permits a site for one user, all other users are automatically permitted to access the site.

To assure the best accuracy in this environment, all clients must be filtered by the same policy, and that policy must use a single category set 24 hours a day, seven days a week.

Additionally, any time you modify your Websense filtering policies, be sure to clear the cache by installing the firewall policy, or by restarting the firewall, or by entering **fw tab -x -t ipufp\_cache** at the firewall machine. Otherwise, the cache might permit sites that should be blocked by the revised policy.

## Two-Request Caching

Two-request caching is called *VPN-1 Pro/Express (two-request) caching* in FireWall-1 NGX, and *VPN-1 and FireWall-1 (two-request) caching* in FireWall-1 NG and FireWall-1 NG with AI.

Two-request caching is not supported by the Websense UFP Server. If you select two-request caching, caching behavior will be as described for one-request caching.



# Configuring FireWall-1 NG, NG with AI, and NGX

In addition to defining Websense filtering policies and assigning them to the appropriate clients (as described in the *Administrator's Guide* for Websense Enterprise/Web Security Suite), you must set up FireWall-1 with the necessary objects and rules. In describing these objects and rules, this chapter assumes that you are familiar with general FireWall-1 concepts.

The following tasks must be completed before you begin to configure FireWall-1 to communicate with the Websense software:

- ◆ Both FireWall-1 and Websense Enterprise/Web Security Suite must already be installed and running.
- ◆ An Object for the firewall itself must exist. Consult the FireWall-1 documentation for information about this procedure.
- ◆ Network Objects that represent your network topology (as needed for your filtering goals) must exist. Consult the FireWall-1 documentation for information about this procedure.
- ◆ A Network Object for the machine running the Websense Filtering Service must exist. Consult the FireWall-1 documentation for information about this procedure.

Configuring FireWall-1 NG, FireWall-1 NG with AI, and FireWall-1 NGX for Websense content filtering involves the following procedures:

- ◆ Creating an OPSEC™ Application Object for the Websense UFP Server.
- ◆ Creating URI Resource Objects for the dictionary categories that the Websense software sends to FireWall-1.
- ◆ Defining rules that govern how FireWall-1 behaves when it receives a response from the Websense software.

The following optional configuration procedures are also described in this chapter:

- ◆ Configuring both the Websense software and FireWall-1 to use Secure Internal Communication (SIC), rather than the default clear communication.
- ◆ Restoring clear communication.
- ◆ Configuring for Enhanced UFP Performance (*FireWall-1 NG with Application Intelligence* and *FireWall-1 NGX* only). Make sure you have configured FireWall-1 for Websense content filtering before this procedure.



#### Note

The procedures and illustrations in this chapter are based on FireWall-1 NGX. If you are using FireWall-1 NG or FireWall-1 NG with Application Intelligence (AI), you may notice slight differences in the appearance of screens and the names of fields. Any significant difference between versions is noted in the text.

---

## Creating an OPSEC Application Object

---

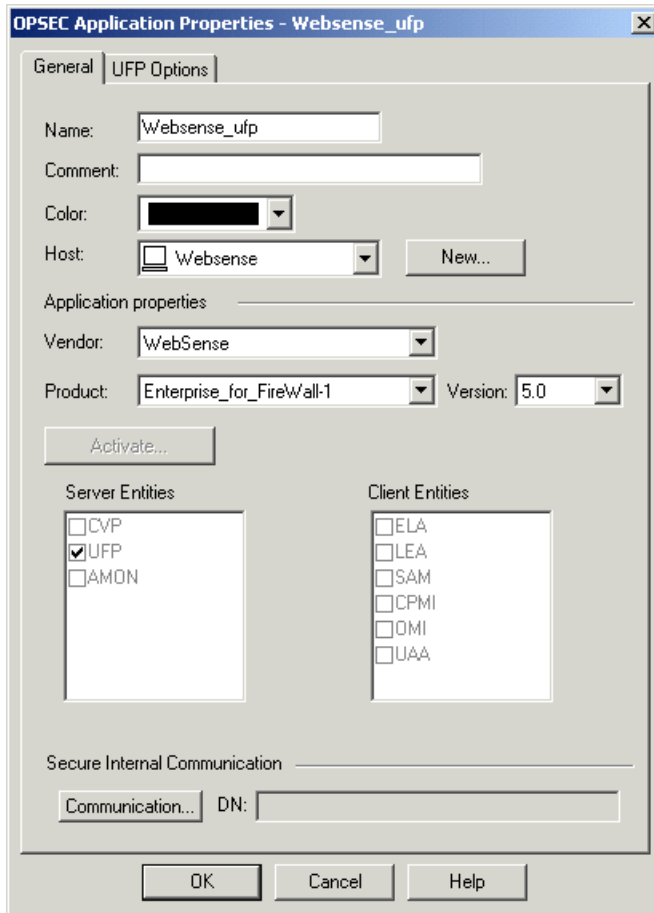
Create an OPSEC Application Object for the Websense UFP Server with the following settings.

1. On the FireWall-1 machine, open the Check Point SmartDashboard™ (*Policy Editor* in earlier versions).
2. If you have not already done so, create a Network Object (**Manage** > **Network Objects** > **New** > **Node** > **Host**) for the machine on which the Websense Filtering Service is running. See your FireWall-1 documentation for assistance. (This object is required only if Websense software is running on a separate machine behind the firewall, as recommended.)
3. Select **Manage** > **Servers and OPSEC Applications** to open the **Servers and OPSEC Applications** dialog box.
4. Click **New**, and then choose **OPSEC Application** from the drop-down list.



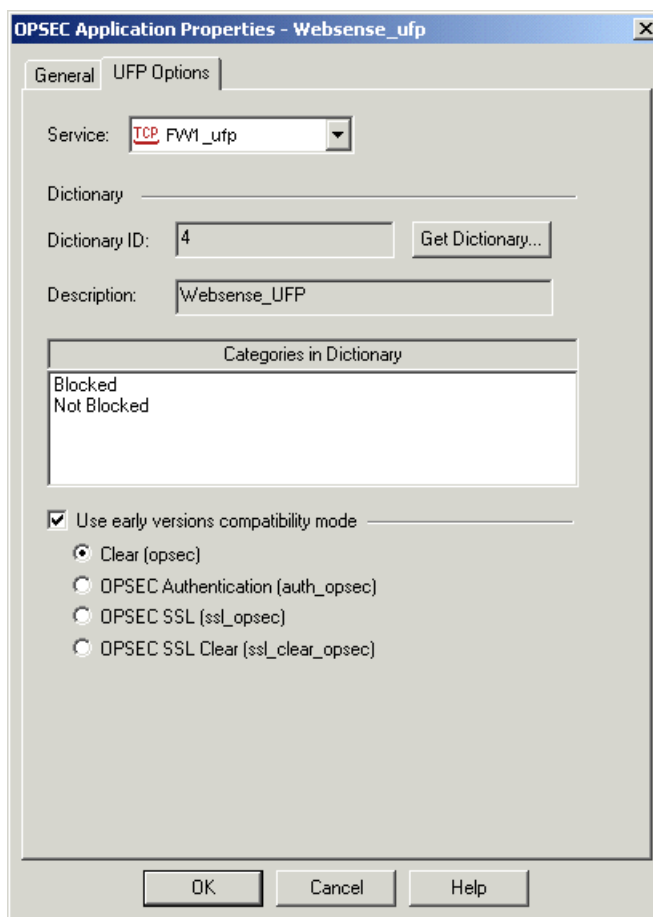
5. In the **General** tab of the **OPSEC Application Properties** dialog box, make the following entries or selections:

Field	Description
Name	Enter a descriptive name, such as Websense_ufp ( <i>remember this name for later use</i> ).
Comment	Enter any desired description for this object.
Color	Select the color desired for displaying this object in SmartDashboard (Policy Editor in earlier versions).
Host	Select the Network Object, created previously, that identifies the machine on which the Websense Filtering Service is running.  If you have not yet created this object, click the New button to create it. See your FireWall-1 documentation for more information.
Vendor	Select WebSense.
Product	The value in this field is not used in creating an OPSEC Application Object and does not need to be changed. (Enterprise_for_FireWall-1 is the default for NGX.)
Version	The value in this field is not used in creating an OPSEC Application Object and does not need to be changed. (5.0 is the default for NGX.)
Server Entities	UFP should be checked. (This value is selected by default when you select WebSense in the Vendor field, and cannot be changed).



OPSEC Application Properties – General tab

6. Go to the **UFP Options** tab.



OPSEC Application Properties – UFP Options tab

7. Check the **Use early versions compatibility mode** option (**Backwards Compatibility** in earlier versions).
8. Select **Clear (opsec)**.
9. Click **Get Dictionary**.  
The Websense software provides FireWall-1 with a dictionary of two categories: **Blocked** and **Not Blocked**. The full set of Websense categories is configured via the Websense Manager.
10. Click **OK**.

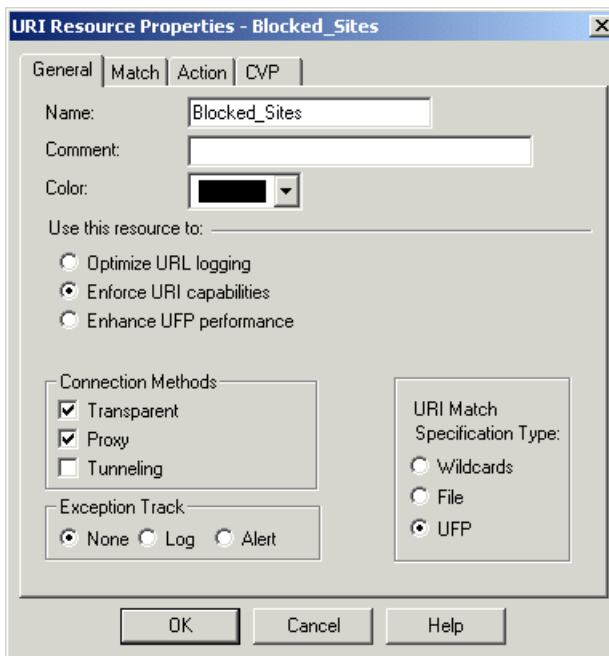
11. Close the **Servers and OPSEC Applications** dialog box.
12. Select **Policy > Install** to install the policy on the firewall. (See your FireWall-1 documentation if you need additional information.)

## Creating Resource Objects

Create a Resource Object to define a Uniform Resource Identifier (URI) that uses the HTTP protocol. This URI identifies the Websense dictionary category “Blocked.”

1. Select **Manage > Resources**.  
The **Resources** dialog box appears.
2. Click **New**, and choose **URI** from the submenu to display the **URI Resource Properties** dialog box.
3. In the **General** tab, make the following entries or selections:

Field	Description
Name	Name of this URI Resource Object (e.g., Blocked_Sites).
Comment	Optional description.
Color	Indicates the color used for this URI Resource Object’s icon.
Use this resource to	Select Enforce URI capabilities. Selecting this option will enable all other functionality of the URI resource: for example, you will be able to configure CVP checking on the CVP tab. All basic parameters, defining schemes, hosts, paths, and methods will apply, and the URL will be checked for these.
Connection Methods	Select both Transparent and Proxy (default).
Exception Track	Select the desired method for tracking exceptions. See your FireWall-1 documentation for more information.
URI Match Specification Type	Select UFP.

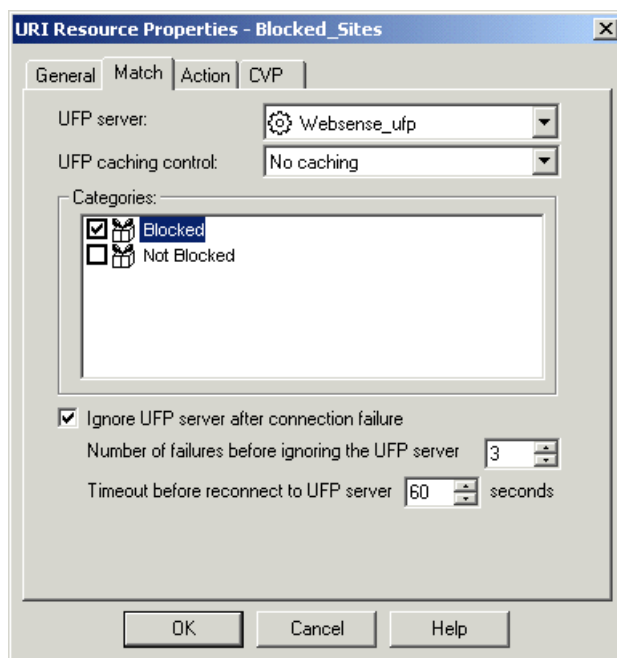


URI Resource Properties – General tab

4. Go to the **Match** tab and make the following entries or selections:

Field	Description
UFP server	Select the OPSEC Application Object that was created for the Websense UFP Server in <i>Creating an OPSEC Application Object</i> , page 224.
UFP caching control	Select a caching option. No caching is the recommended setting for most networks. For detailed information about caching options, see <i>Caching</i> , page 219.

Field	Description
Categories	Check <i>Blocked</i> .
Ignore UFP server after connection failure	<ul style="list-style-type: none"> <li>• Check this option to permit full HTTP and FTP access when the Websense Filtering Service is not running. Dependent fields allow you to set the number of times FireWall-1 will try to contact the Websense software before ignoring it, and the length of time FireWall-1 will ignore the Websense software before attempting to reconnect.</li> <li>• Leave this option unchecked to block all HTTP and FTP access when the Websense Filtering Service is not running.</li> </ul>



URI Resource Properties – Match tab

5. Click **OK**.
6. Close the **Resources** dialog box.
7. Select **Policy > Install** to install the policy on the firewall. (See your FireWall-1 documentation if you need additional information.)

## Defining Rules

---

The following section describes a content filtering scenario and its configuration. Included is information about the objects and rules that are needed to implement the suggested configuration.

The configuration described here assumes that all clients have their default route set to the firewall and do not proxy to the firewall. This configuration also assumes that the recommended network configuration is being used: Websense software is running on a separate machine, behind the firewall, and caching is disabled.

In this scenario, FireWall-1 denies access to any site that the Websense software indicates is Blocked, and allows access to any site that the Websense software indicates is Not Blocked. The actual sites blocked may vary according to the workstation making the request.

For example, in Websense Manager you might define the **Global** policy to always use a category set that blocks access to all categories except the **Travel** and **Business and Economy** categories. In this case, let the **Global** policy apply to most workstations.

In addition, you could define a separate, more liberal policy that blocks only those categories considered a liability risk, such as Adult Material and Gambling. This policy might be called Management, and would be assigned to the workstations used by top managers.

When FireWall-1 receives an HTTP request, it sends the Websense software the address of the requested site as well as the IP address of the workstation requesting the site. Suppose the requested site is CNN, which Websense software categorizes as **News and Media**. If the CNN site was requested from a top manager's workstation, the Websense software would indicate that the site was **Not Blocked** because top managers are assigned the more liberal Management policy that you defined in Websense Manager. Upon receiving the **Not Blocked** response, FireWall-1 would allow the site according to the Rule 2, defined below.

If the CNN site was requested by an accounting clerk's workstation, the Websense software would indicate that the site was Blocked because that workstation is governed by the **Global** policy, which you defined to block the **News and Media** category (along with most others). As a result, FireWall-1 would deny access according to Rule 1, defined below.

Any time a workstation requested a site that the Websense software does not categorize, the Websense software would indicate that it is not in the database. FireWall-1 would allow access to the site according to Rule 2, defined below.

To implement this type of strategy, use Websense Manager to define policies that block the appropriate categories, and assign them to the desired workstations or directory objects. Then define rules in FireWall-1 to block access to any site that the Websense software indicates is Blocked.

Implementing this configuration in FireWall-1 requires creating one URI Resource Object and one Network Object, and defining two rules.

Create a URI Resource Object for the Blocked category as described in [Creating Resource Objects, page 228](#). In this example, the URI Resource Object is called Blocked\_Sites because the Websense software is set up to block sites that are not required for business purposes.

Create a Network Object that encompasses all machines on the internal network. (We are assuming in this example that everyone in the company is on the internal network.) For this example, the Network Object is called Internal\_Network.

Next, add the rules to the Security Rules Base. Remember that the sequence of the rules is important, because FireWall-1 evaluates the rules sequentially, from top to bottom.

**RULE 1:** This rule blocks access to undesirable websites. Add the new rule at an appropriate location in the Rule Base:

**Name:** (NGX only) Enter a descriptive name for the rule, such as Websense Block  
**Source:** Add/Internal\_Network  
**Destination:** Any (default)  
**Service:** Add with Resource/HTTP->Blocked\_Sites  
**Action:** Reject  
**Track:** None  
**Install On:** Policy Targets  
**Time:** Any (default)  
**Comment:** (NGX only) Enter a more detailed description of the rule.

**RULE 2:** The second rule allows access to all other websites. Add the second rule *after* Rule 1.

**Name:** (NGX only) Enter a descriptive name for the rule, such as Websense Allow  
**Source:** Add/Internal\_Network



**Destination:** Any (default)

**Service:** Add/HTTP

**Action:** Accept

**Track:** None

**Install On:** Policy Targets

**Time:** Any (default)

**Comment:** (NGX only) Enter a more detailed description of the rule.

The following illustrations shows what the Security Rule Base might look like after you define these rules.

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION
1	vWebsense Block	Internal_Network	* Any	* Any Traffic	HTTP http->Blocked_Sites	reject
2	vWebsense Allow	Internal_Network	* Any	* Any Traffic	TCP http	accept
3	Clean-up Rule	* Any	* Any	* Any Traffic	* Any	drop

	ACTION	TRACK	INSTALL ON	TIME	COMMENT
_Sites	reject	- None	* Policy Targets	* Any	Blocks websites that Websense categorizes as Blocked.
	accept	- None	* Policy Targets	* Any	Allows access to all other websites.
	drop	- None	* Policy Targets	* Any	

Security Rule Base – Deny Blocked Categories Policy

After defining the two rules described above, **Verify** and **Install** the policy from the **Policy** menu. (See your FireWall-1 documentation for more information.)



**Important**

For normal operation, set **Track** to **None** for the Websense rules in order to disable logging in FireWall-1. When logging is enabled for these rules, the log files will become very large, and will adversely affect performance. Configure other options in the **Track** field only when testing and troubleshooting.

## Establishing Secure Internal Communication (SIC)

---

If Websense Enterprise is integrated with FireWall-1 NG Feature Pack 1 or later, you may configure both programs to use Secure Internal Communication (SIC). A secure connection requires that communication between FireWall-1 and the Websense UFP Server be authenticated before any data is exchanged.



### Note

The use of SIC with Websense Enterprise/Web Security Suite creates performance problems and is not recommended for networks with more than 100 users.

---

After installing the Websense Filtering Service, establish an SIC trust between FireWall-1 and the Websense software by performing the procedures detailed in the following sections:

- ◆ Configure the OPSEC Application Object for the Websense UFP Server within FireWall-1 to use Secure Internal Communication.
- ◆ Configure the Websense software to use Secure Internal Communication.
- ◆ Update the OPSEC Application Object within FireWall-1 to receive secure communications from the Websense software.

## Prerequisites

The following must be completed before you begin to configure FireWall-1 to communicate with the Websense filtering software:

- ◆ Both FireWall-1 and Websense Enterprise/Web Security Suite must already be installed and running.
- ◆ An Object for the firewall itself must exist. Consult the FireWall-1 documentation for information about this procedure.
- ◆ Network Objects that represent your network topology (as needed for your filtering goals) must exist. Consult the FireWall-1 documentation for information about this procedure.
- ◆ You must create the OPSEC Application Object for the Websense UFP Server before the Websense software can establish Secure Internal Communication (SIC). If you have not already done this, see the

procedures in [Creating an OPSEC Application Object](#), page 224 for instructions.



**Note**

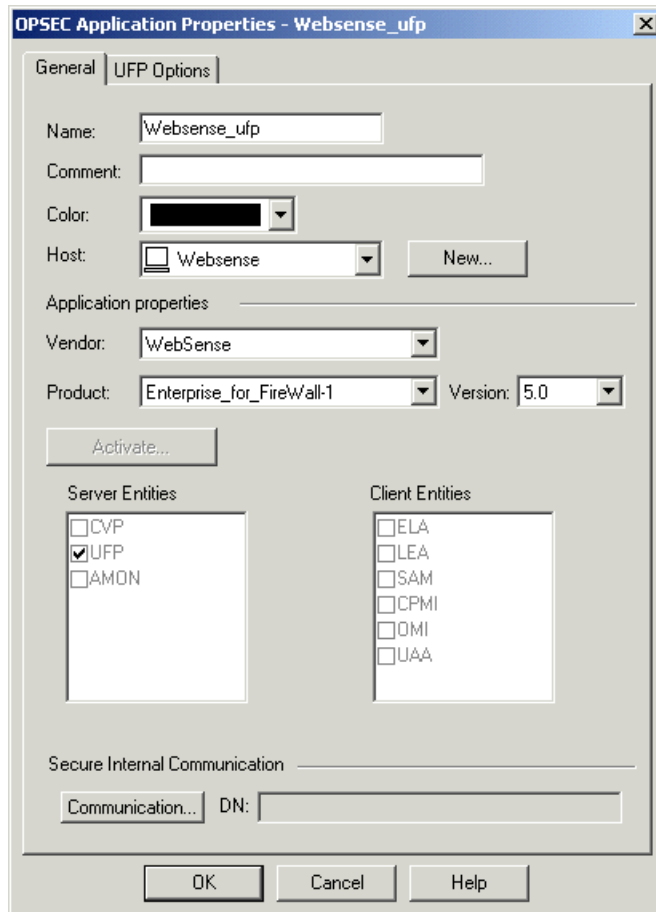
DO NOT perform the procedures found in this section if you are using an earlier version of FireWall-1 (before FireWall-1 NG Feature Pack 1).

---

## Configuring FireWall-1 to Use SIC

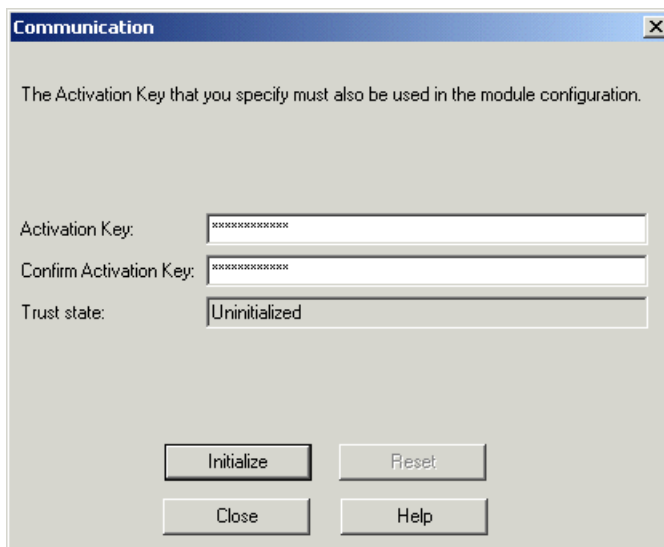
1. On the FireWall-1 machine, open the SmartDashboard (*Policy Editor* in earlier versions).
2. Choose **Manage > Servers and OPSEC Applications**.
3. Double-click on the OPSEC Application Object you created for the Websense UFP Server in [Creating an OPSEC Application Object](#), page 224.

The **OPSEC Application Properties** dialog box for this object opens.



OPSEC Application Properties – General tab

- Click **Communication** to display the **Communication** dialog box.



Communication Dialog Box

- Enter and confirm an **Activation Key** (password) for communication between the Websense Filtering Service and FireWall-1. (*Remember* this password for later use.)
- Click **Initialize**.  
The **Trust state** field must show **Initialized but trust not established**.
- Click **Close** to return to the **OPSEC Application Properties** dialog box.
- Click **OK**.
- Close the **Servers and OPSEC Applications** dialog box.
- Select **Policy > Install** to install the policy on the firewall. (See your FireWall-1 documentation if you need additional information.)

## Configuring the Websense Software to Use SIC

Use this procedure to obtain a Secure Internal Communication (SIC) certificate from FireWall-1, and configure the Websense software to use it. After you complete this procedure, the Websense software will send this certificate every time it communicates with FireWall-1.

- Go to the machine on which the Websense Filtering Service is running.

2. At a command prompt, go to the directory where the FireWall-1 integration files were installed:
  - **Windows:** \Websense\bin
  - **Linux:** /Websense/bin
  - **Solaris:** /Websense/bin/FW1
3. Enter the following command:

```
opsec_pull_cert -h <host> -n <object> -p <password> -o <path>
```

Variable	Description
<host>	The IP address or machine name of the computer on which the FireWall-1 SmartCenter™ Server (Management Server) is installed. This may be the same machine containing the FireWall Module or a different machine.
<object>	The name of the OPSEC Application Object created for the Websense UFP Server.
<password>	The activation key you entered for the named OPSEC Application Object.
<path>	Path to the output certificate file (opsec.p12). This must be expressed as a complete path in the command. <ul style="list-style-type: none"> <li>• If the <b>OPSECDIR</b> variable already exists, the default path is \$OPSECDIR/opsec.p12.</li> <li>• If the <b>OPSECDIR</b> variable does not exist, the opsec.p12 file will be created in the same folder as the opsec_pull_cert.exe file (\Websense\bin or /Websense/bin/FW1).</li> </ul>

This command contacts the firewall and downloads the Secure Internal Communication (SIC) certificate that authorizes Websense software to communicate with FireWall-1, and saves the certificate in a file called opsec.p12. The command line displays information similar to the following example:

```
opsec_pull_cert -h 10.201.254.245 -n Websense_UFP -p
firewall -o "C:\Program Files\Websense\bin\opsec.p12"
The full entity sic name is:
CN=Websense_UFP,0=fw1_server..dwz26v
Certificate was created successfully and written to
"opsec.p12".
```

4. Write down the SIC name displayed by the `opsec_pull_cert` command. In the example above, the SIC name is:

```
CN=Websense_UFP,0=fw1_server..dwz26v
```

5. Open the `ufp.conf` file, located in `\Websense\bin` (Windows and Linux) or `/Websense/bin/FW1` (Solaris). The default file should contain the following information:

```
ufp_server port 18182
#ufp_server auth_port 18182
#opsec_sic_policy_file ufp_sic.conf
#opsec_sic_name "place_holder_for_opsec_SIC_name"
#opsec_sslca_file opsec.p12
```

The first line is used for clear communication; the remaining lines are used for Secure Internal Communication. If the file does not contain the lines for Secure Internal Communication shown above, type them in.

6. To enable secure communication, comment out the first line and remove the comment symbols (`#`) from the remaining four lines.
7. On the `opsec_sic_name` line, replace the placeholder with the SIC name recorded in [Step 4](#). The name must be enclosed in quotation marks. For example:

```
opsec_sic_name "CN=Websense_UFP,0=fw1_server..dwz26v"
```

8. Save and close the `ufp.conf` file.
9. Stop and restart the Websense UFP Server:
  - **Windows:** Use the **Services** window in the Windows Control Panel (see [Windows](#), page 186).
  - **Solaris or Linux:** Use the `WebsenseAdmin restart` command (see [Solaris and Linux](#), page 188).

## Updating the OPSEC Application Object

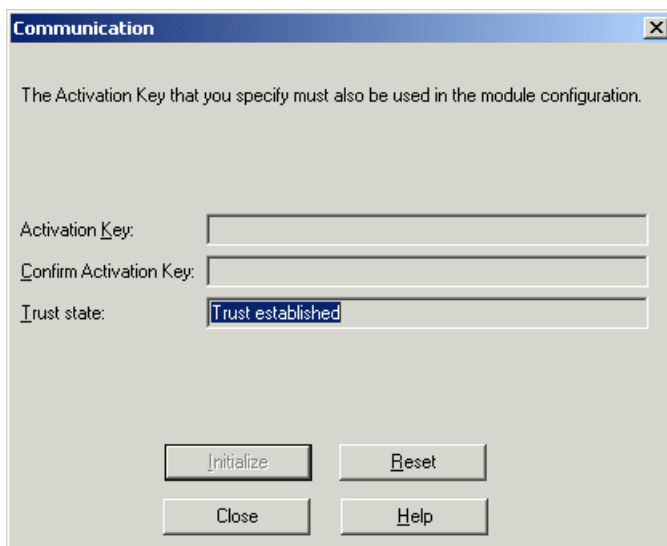
After the Websense software has been configured to use Secure Internal Communication, you must update the OPSEC Application Object created for the Websense UFP Server.

1. On the FireWall-1 machine, open the SmartDashboard (*Policy Editor* in earlier versions).
2. Choose **Manage > Servers and OPSEC Applications**.

3. Double-click on the OPSEC Application Object you created for the Websense UFP Server in *Creating an OPSEC Application Object*, page 224.

The **OPSEC Application Properties** dialog box for this object opens.

4. Click the **Communication** button.
5. Verify that the **Trust state** field shows **Trust established**.

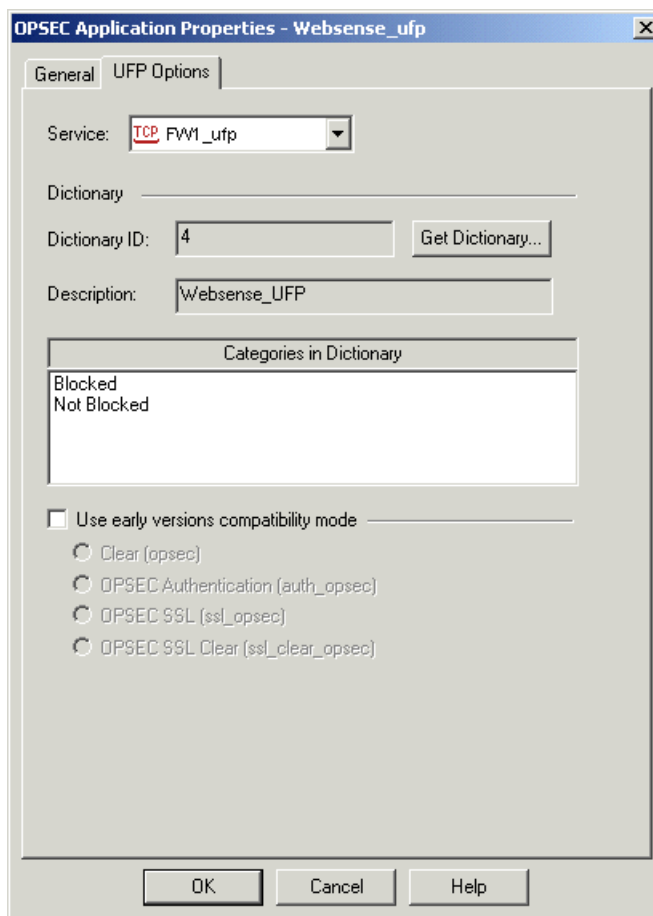


Communication Dialog Box – Trust established

6. Click **Close** to return to the **OPSEC Application Properties** dialog box.
7. Click **OK**.
8. Close the **Servers and OPSEC Applications** dialog box.
9. Select **Policy > Install** to install the policy on the firewall. (See your FireWall-1 documentation if you need additional information.)
10. Open the OPSEC Application Object created for the Websense UFP Server again.



11. Go to the **UFP Options** tab of the **OPSEC Application Properties** dialog box for this object.



OPSEC Application Properties – UFP Options tab,  
FireWall-1 configured for SIC

12. Make sure the **Use early versions compatibility mode** check box is *not* selected. (This field was called **Use backwards compatibility mode** in earlier versions.)
13. Click **Get Dictionary**.

The Websense software provides FireWall-1 with a dictionary of two categories: *Blocked* and *Not Blocked*. The full set of Websense categories is configured through the Websense Manager.



### Important

Before continuing, make sure the **Use early versions compatibility mode** check box is *not* selected.

---

14. Click **OK**.
15. Close the **Servers and OPSEC Applications** dialog box.
16. Select **Policy > Install** to install the policy on the firewall. (See your FireWall-1 documentation if you need additional information.)

The SIC trust between the Websense software and FireWall-1 has now been established.

## Restoring Clear Communication

---

To restore clear communication (*early versions compatibility* mode in FireWall-1) on a system configured for Secure Internal Communication (SIC):

1. Go to the machine on which the Websense Filtering Service is running.
2. Navigate to the directory where the FireWall-1 integration files were installed:
  - **Windows:** \Websense\bin
  - **Linux:** /Websense/bin
  - **Solaris:** /Websense/bin/FW1
3. Open the `ufp.conf` file in any text editor.

When FireWall-1 is configured for Secure Internal Communication (SIC) this file contains the following information:

```
#ufp_server port 18182
ufp_server auth_port 18182
opsec_sic_policy_file ufp_sic.conf
opsec_sic_name "place_holder_for_opsec_SIC_name"
opsec_sslca_file opsec.pl2
```

Note that if SIC was fully configured, the contents of the quotation marks in line 4 will have been replaced with an actual `opsec_SIC_name`, such as `CN= Websense_UFP , O=fw1_server . .dwz26v`.

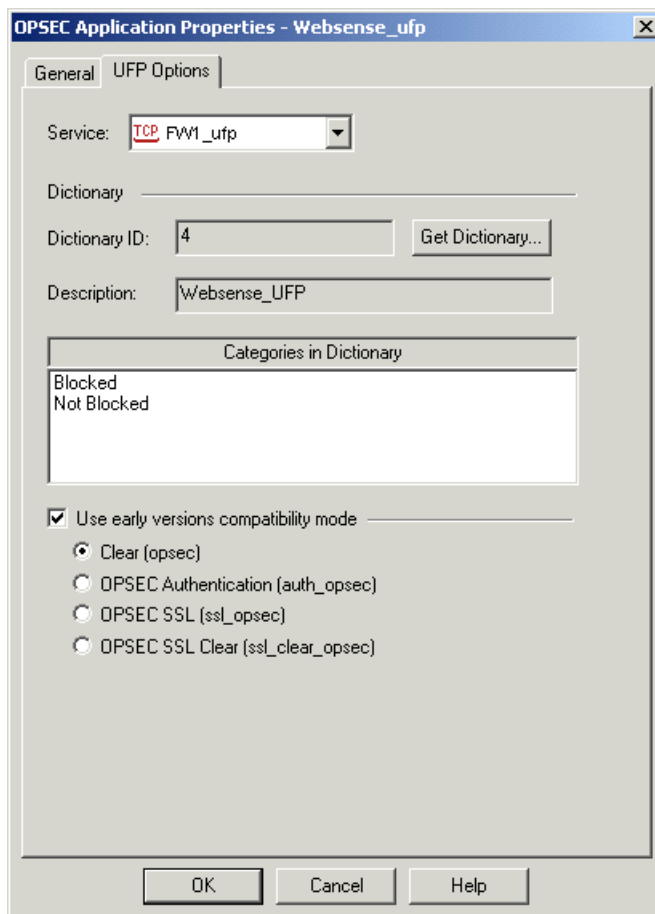
4. To restore clear communication, remove the comment symbol (#) from the first line, and comment out the remaining lines.

The information should now read:

```
ufp_server port 18182
#ufp_server auth_port 18182
#opsec_sic_policy_file ufp_sic.conf
#opsec_sic_name "place_holder_for_opsec_SIC_name"
#opsec_sslca_file opsec.p12
```

5. Save the file.
6. Stop and start the Websense UFP Server:
  - **Windows:** Use the **Services** window in the Windows Control Panel (see *Windows*, page 186).
  - **Solaris or Linux:** Use the `WebsenseAdmin restart` command (see *Solaris and Linux*, page 188).
7. On the FireWall-1 machine, open the SmartDashboard (*Policy Editor* in earlier versions).
8. Choose **Manage > Servers and OPSEC Applications** and double-click on the OPSEC Application Object for the Websense UFP Server.  
The **OPSEC Application Properties** dialog box for this object opens.
9. Click **Communication** to display the **Communication** dialog box.
10. Click **Reset** to revoke the SIC certificate and stop SIC.  
A confirmation dialog box appears.
11. Click **Yes** to continue.
12. Click **Close** to return to the **OPSEC Application Properties** dialog box.

13. Go to the **UFP Options** tab.



OPSEC Application Properties – UFP Options tab, FireWall-1 configured for clear communication

14. Check the **Use early versions compatibility mode** option (**Backwards Compatibility** in earlier versions of FireWall-1 NG).
15. Select **Clear (opsec)**.
16. Click **Get Dictionary**.  
The Websense software provides FireWall-1 with a dictionary of two categories: **Blocked** and **Not Blocked**. The full set of Websense categories is configured via the Websense Manager.
17. Click **OK**.

18. Close the **Servers and OPSEC Applications** dialog box.
19. Select **Policy > Install** to install the policy on the firewall. (See your FireWall-1 documentation if you need additional information.)

## Enhanced UFP Performance

---

Check Point has improved the performance of the UFP Server in FireWall-1 NG with Application Intelligence (AI) and FireWall-1 NGX with the Enhanced UFP Performance feature. This feature, also known as QuickUFP, increases the amount of traffic that the Websense software and FireWall-1 can filter while reducing CPU load.

Configuring for Enhanced UFP Performance requires the proper settings in both Websense Enterprise/Web Security Suite and FireWall-1. In order to use the Enhanced UFP Performance feature, clear communication is required between the Websense software and FireWall-1.



### Note

Make sure you have configured FireWall-1 for content filtering with the Websense software before completing the following procedures.

---

## Websense Configuration

Before configuring FireWall-1 for Enhanced UFP Performance, open the `ufp.conf` file and check to make sure the Websense software is configured for clear communication:

1. Go to the machine on which the Websense Filtering Service is running.
2. Navigate to the directory where the FireWall-1 integration files were installed:
  - **Windows:** `\Websense\bin`
  - **Linux:** `/Websense/bin`
  - **Solaris:** `/Websense/bin/FW1`
3. Open the `ufp.conf` file in any text editor.

To be configured for clear communication, the file must contain the following line:

```
ufp_server port 18182
```

Additional lines that appear in this file are used for Secure Internal Communication, and must be commented out using the comment symbol (#):

```
#ufp_server auth_port 18182
#opsec_sic_policy_file ufp_sic.conf
#opsec_sic_name "place_holder_for_opsec_SIC_name"
#opsec_sslca_file opsec.pl2
```

4. Edit the file if necessary.
5. Save and close the `ufp.conf` file.
6. Stop and restart the Websense UFP Server:
  - **Windows:** Use the **Services** window in the Windows Control Panel (see [Windows](#), page 186).
  - **Solaris or Linux:** Use the `WebsenseAdmin restart` command (see [Solaris and Linux](#), page 188).

## FireWall-1 Configuration

To configure for Enhanced UFP Performance in FireWall-1, you must do the following:

- ◆ Configure the OPSEC Application Object for the Websense UFP Server to operate in *early versions compatibility mode* (previously known as *backwards compatibility mode*) for clear communication. Clear communication is the default for FireWall-1 NG with AI and FireWall-1 NGX.
- ◆ Configure the URI Resource Object that identifies the Websense dictionary category “Blocked” for Enhanced UFP Performance.

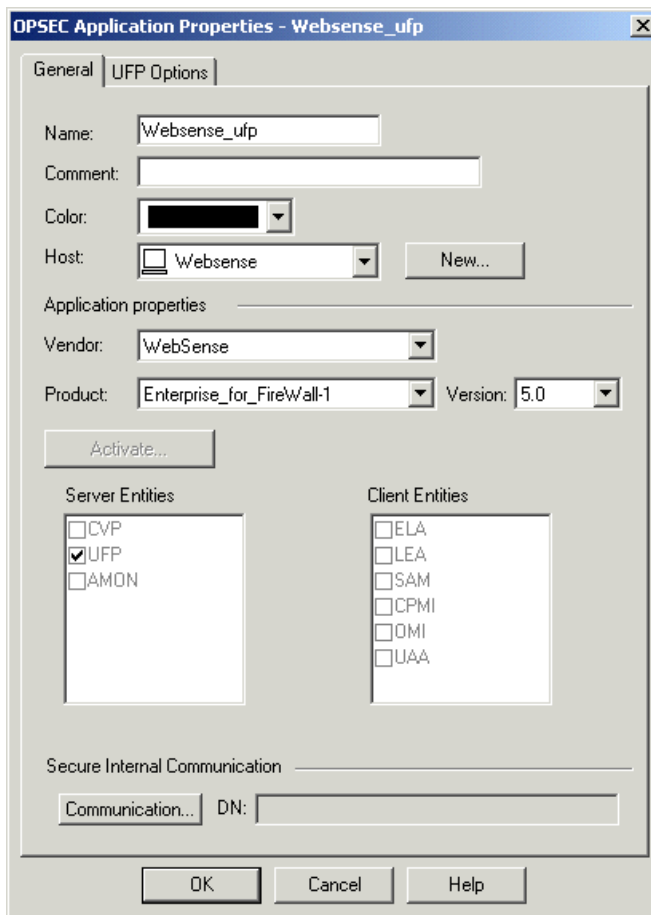
### Early Versions Compatibility Mode

To configure the previously created OPSEC Application Object for the Websense UFP Server to operate in early versions compatibility mode (clear communication) for Enhanced UFP Performance:

1. On the FireWall-1 machine, open the SmartDashboard (*Policy Editor* in earlier versions).

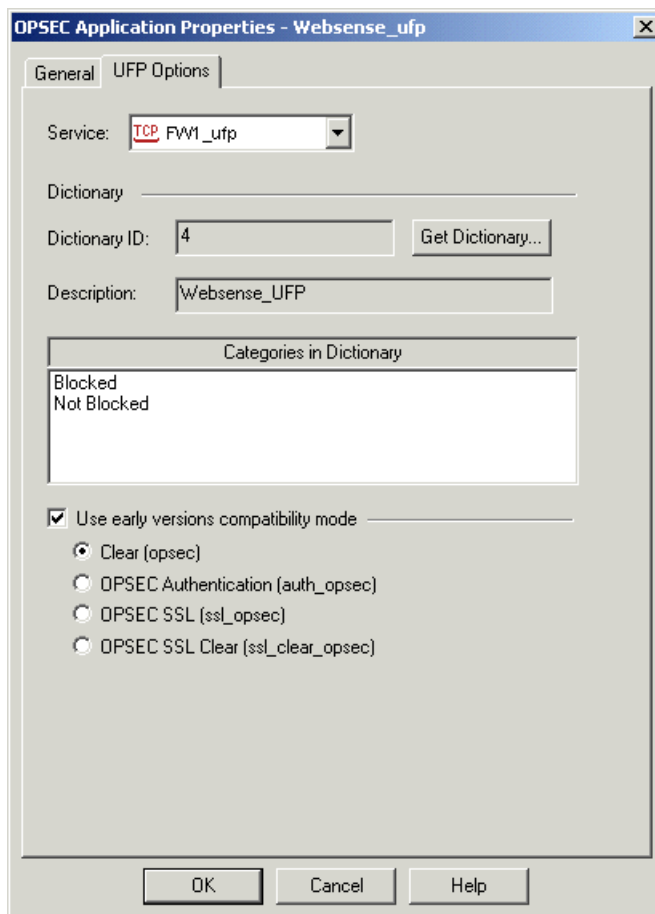
2. Choose **Manage > Servers and OPSEC Applications**.
3. Double-click on the OPSEC Application Object you created for the Websense UFP Server in *Creating an OPSEC Application Object*, page 224.

The **OPSEC Application Properties** dialog box for this object opens.



OPSEC Application Properties – General tab

4. Select the **UFP Options** tab.



OPSEC Application Properties – UFP Options tab, configured for Enhanced UFP Performance

5. Select **Use early versions compatibility mode (Backwards Compatibility)** in earlier versions).
6. Select **Clear (opsec)**.
7. Click **OK**.
8. Close the **Servers and OPSEC Applications** dialog box.
9. Select **Policy > Install** to install the policy on the firewall. (See your FireWall-1 documentation if you need additional information.)



## Enhanced UFP Performance

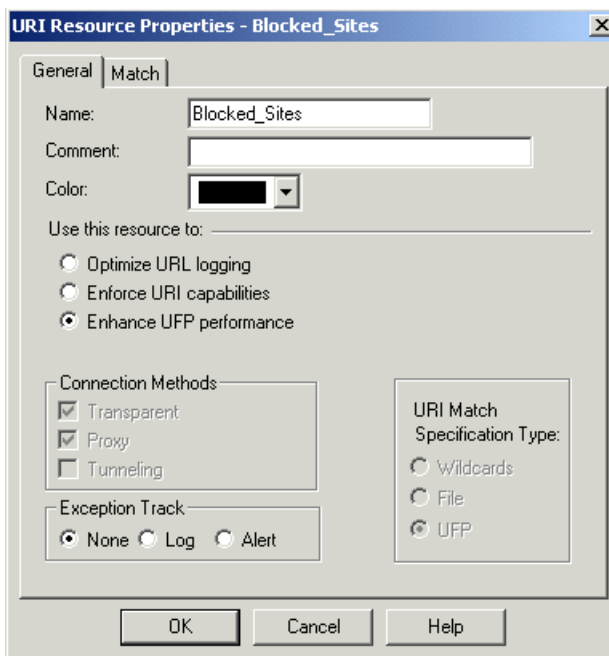
To configure the previously created URI Resource Object that identifies the Websense Dictionary category “Blocked” for Enhanced UFP Performance:

1. On the FireWall-1 machine, open the SmartDashboard (*Policy Editor* in earlier versions).
2. Select **Manage > Resources**.

The **Resources** dialog box appears.

3. Double-click on the Resource Object you created for the Websense Dictionary category “Blocked” in [Creating Resource Objects](#), page 228.

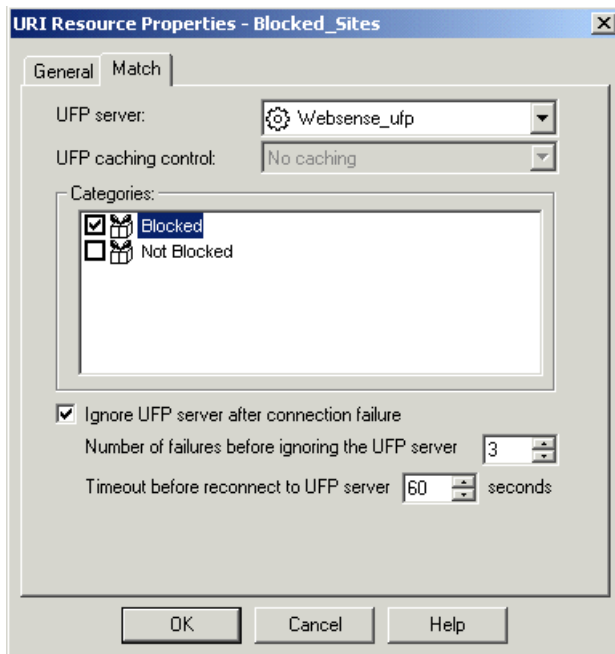
The **URI Resource Properties** dialog box for this resource opens.



URI Resource Properties – General tab,  
configured for Enhanced UFP Performance

4. In the **General** tab, select **Enhance UFP performance**.

5. Select the **Match** tab.



URI Resource Properties – Match tab,  
configured for Enhanced UFP Performance

6. Reselect the OPSEC Application Object for the Websense UFP Server in the **UFP server** field. (In this example, the object entitled **Websense\_ufp**.)
7. Uncheck and then recheck the **Blocked** category, and click **OK**.
8. Close the **Resources** dialog box.
9. Select **Policy > Install** to install the policy on the firewall. (See your FireWall-1 documentation if you need additional information.)

In some cases, it might be desirable to configure the Network Agent to inspect all packets with a network interface card (NIC) that has been configured for *stealth mode*. A NIC in stealth mode has no IP address and cannot be used for communication. The advantages for this type of configuration are security and network performance. Removing the IP address prevents connections to the interface from outside and stops unwanted broadcasts.

## Configuring for Stealth Mode

---

If the Network Agent is configured for a stealth mode NIC, the installation machine must be multihomed. In remote installations of Network Agent, a second, TCP/IP-capable interface must be configured to communicate with the central Websense software for filtering and logging purposes.

Stealth mode NICs display normally during Network Agent installation. You may test a stealth mode NIC for traffic visibility and select it for Network Agent to use to monitor internet traffic. When installing on Windows, stealth mode interfaces do not display as a choice for Websense communications.



### Important

In Solaris and Linux, stealth mode NICs appear together with TCP/IP-capable interfaces and must not be selected for communication.

---

Make sure you know the configuration of all the interfaces in the machine before attempting an installation.

## Windows

Stealth mode for the Network Agent interface is supported in Windows.

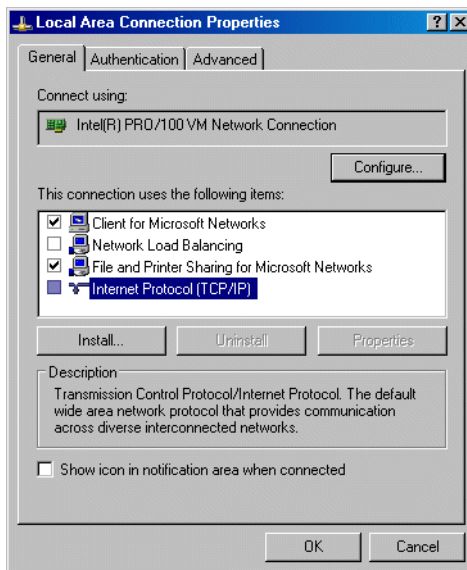
To configure a NIC for stealth mode:

1. From the Start menu, select **Settings > Network and Dial-up Connection**.

A list of all the interfaces active in the machine is displayed.

2. Select the interface you want to configure.
3. Select **File > Properties** or right-click and select **Properties** from the pop-up menu.

A dialog box displays the connections properties of the interface you have chosen.



Interface Connections Properties

4. Clear the **Internet Protocol (TCP/IP)** checkbox.
5. Click **OK**.

## Solaris or Linux

To configure a NIC for stealth mode in Solaris or Linux, you must disable the Address Resolution Protocol (ARP), which severs the link between the IP address and the MAC address of the interface.

### Solaris

- ◆ To configure a NIC for stealth mode, run the following from a command prompt:

```
ifconfig <interface> plumb -arp up
```

- ◆ To return the NIC to a normal mode, run the following from a command prompt:

```
ifconfig <interface> plumb arp up
```

### Linux

- ◆ To configure a NIC for stealth mode, run the following from a command prompt:

```
ifconfig <interface> -arp up
```

- ◆ To return the NIC to a normal mode, run the following from a command prompt:

```
ifconfig <interface> arp up
```



#### Important

Network Agent can work with a stealth mode NIC only if the interface retains its old IP address in the Solaris or Linux system configuration file.

---



## APPENDIX B | Troubleshooting

You may encounter a situation while installing Websense Enterprise or Web Security Suite and configuring Check Point FireWall-1 that is not addressed in the previous chapters. This appendix provides troubleshooting information for installation and initial configuration issues that have been called in to Websense Technical Support. Please check this chapter for information about the problem you are having before you contact Technical Support. For issues not related to installation or communication between Websense software and your integration product, see the *Administrator's Guide* for Websense Enterprise/Web Security Suite.

If you still need to contact Technical Support, please see [Appendix C: Technical Support](#) for contact information. The situations addressed in this chapter are as follows:

- ◆ I made a mistake during installation.
- ◆ I installed using a non-English language version of the Websense installer, and the Language Pack installer did not automatically start.
- ◆ I forgot my Websense Policy Server password.
- ◆ Where can I find download and error messages?
- ◆ The Master Database does not download.
- ◆ Policy Server fails to install.
- ◆ I upgraded my Websense software, and configured users no longer appear under Directory Objects in Websense Manager.
- ◆ Network Agent fails to start on Linux with stealth mode NIC.
- ◆ Windows 9x workstations are not being filtered as expected.
- ◆ I am using Logon Agent and some users are receiving the Websense Global policy.
- ◆ Websense splash screen is displayed, but installer does not launch on Windows 2000.
- ◆ Network Agent cannot communicate with Filtering Service after it has been reinstalled.

- ◆ Websense Dictionary does not load in FireWall-1.
- ◆ I configured FireWall-1 for Enhanced UFP performance, and internet requests are not being filtered.
- ◆ FTP requests are not being blocked by protocol.
- ◆ Users filtered via remote filtering are not receiving block pages.
- ◆ Remote filtering is not working.

## I made a mistake during installation

Run the installation program again. The installer will detect the current installation and allow you to **Add**, **Remove**, or **Repair** Websense components. The **Repair** option does not troubleshoot the installation, but merely reinstalls the files it detects.



### Note

On Windows, you may need to restart the machine before running the installer again.

---

For instructions, see [Modifying an Installation](#), page 163.

## I installed using a non-English Websense installer, but the Language Pack installer did not start

When you install Websense software using one of the non-English installer packages, the Language Pack installer should start after installation of the selected Websense components is complete.

If the Language Pack installer does not start automatically, you can start it manually as follows:

- ◆ **Windows:** Go to the setup folder where you unpacked the Websense installer, and double-click on `SetupLanguagePack.exe`.
- ◆ **Solaris or Linux:** Go to the setup directory where you unpacked the Websense installer, and enter the following command:

```
./installLanguagePack.sh
```

If you are using an English-based UNIX system, you can run the GUI mode of the installer by entering the following command:

```
./installLanguagePack.sh -g
```



Follow the onscreen instructions to complete installation of the Language Pack. Websense components and files on the machine are updated with text in the language you selected.

## I forgot my Websense Policy Server password

Contact Websense Technical Support for assistance. You can find contact information in [Appendix C: Technical Support](#).

## Where can I find download and error messages?

### Windows

Check the Windows Application Event log or `Websense.log` (`Websense\bin`) for any listings about the database download as well as other error or status messages. Access the Application Event log by choosing **Start > Settings > Control Panel > Administrative Tools > Event Viewer**. Expand the **Event Viewer** tree and click **Application Log**.

### Solaris and Linux

The Websense software creates `Websense.log` and `ufpserver.log` (located in `Websense/bin`) when there are errors to record. These log files record error messages and messages pertaining to database downloads. `Websense.log` is located on the Policy Server machine only.

## The Master Database does not download

There are several reasons why you might have difficulty receiving Websense Master Database downloads.

### Subscription Key

Verify that the subscription key is entered correctly and has not expired by going to the **Database Download** screen in Websense Manager (**Server > Settings > Database Download**).

- ◆ Compare the key you received via email or in the Websense package to the key in the **Subscription Key** field (the key is not case sensitive) and correct any errors. You must click **OK** to close the **Settings** dialog box before the key takes effect and enables the database download.

- ◆ Check the date shown in the **Key Expires** field. If this date has passed, contact Websense, Inc., to renew your subscription.
- ◆ It is possible that another rule in the firewall is blocking the download. Create a rule in FireWall-1 at the top of the rulebar that allows all traffic (outbound) from the Websense machine. If this test succeeds, move the rule down systematically until the problematic rule is found.

## Internet Access

The machine running the Filtering Service must have access to the internet via HTTP, and must be able to receive incoming transmissions.

To verify internet access on the Websense Filtering Service machine:

1. Determine whether the Websense software is accessing the internet through a proxy server by checking the **Database Download** screen of the **Settings** dialog box in Websense Manager.
2. If a proxy server is being used, open a web browser.
3. Configure the browser to access the internet with the same proxy settings as those shown in the **Settings** dialog box.
4. Request one of the following addresses:

<http://download.websense.com>

<http://asia.download.websense.com>

<http://europe.download.websense.com>

- If you reach the site, the Websense logo appears, along with a message indicating that it will redirect you to the Websense home page. This means that the Filtering Service's proxy settings are correct, and the Filtering Service should have appropriate HTTP access for downloading.
- If you are not able to reach the download site, and the system requires proxy information, the Filtering Service proxy settings must be corrected.
- If no proxy information is required, use the **nslookup** command (at the command prompt) with the address of your download site to make sure the Filtering Service machine is able to resolve the download location to an IP address. For example:

**nslookup asia.download.websense.com**

If this does not return an IP address, you must set up the machine running Filtering Service to access a DNS server.

If you need assistance, contact Websense Technical Support (see [Appendix C: Technical Support](#) for information).

5. If the Websense software must access the internet through an upstream firewall or proxy server that requires authentication, check the following:
  - The correct user name and password must be entered in the **Database Download** screen of the **Settings** dialog box. Verify spelling and capitalization.
  - The firewall or proxy server must be configured to accept clear text or basic authentication.

## Restriction Applications

Some restriction applications, such as virus scanners or size-limiting applications, can interfere with database downloads. Disable the restrictions relating to the Filtering Service machine and the Websense download location.

## Policy Server fails to install

If you attempt to install Websense software on a machine with insufficient resources (RAM or processor speed), the Policy Server may fail to install. Certain applications (such as print services) can bind up the resources that the installer needs to install the Policy Server. If the Policy Server fails to install, Setup must quit. If you receive the error message: *Could not install current service: Policy Server*, during installation, take one of the following actions:

- ◆ Install Websense software on a different machine. See [System Requirements](#), page 30 for minimum installation requirements.
- ◆ Stop all memory-intensive services running on the machine before attempting another Websense installation.

## I upgraded the Websense software, and configured users no longer appear under Directory Objects in Websense Manager

If you are using Active Directory as your Directory Service, you may find that user names disappear from the list of directory objects in Websense Manager when you upgrade your Websense software. This change occurs if your user names include characters that are not part of the UTF-8 character set.

To support LDAP 3.0, the Websense installer changes the character set from MBCS to UTF-8 during upgrade, so if your user names include non-UTF-8

characters, those characters will not be properly recognized. To fix this problem, try changing the character set back to MBCS.

1. In Websense Manager, go to **Server > Settings > Directory Service**. **Active Directory (Native Mode)** will be selected in the **Directories** pane if you are using Active Directory.
2. Click the **Advanced Settings** button.
3. Click **MBCS** under **Character Set** to change the character set from UTF-8 to MBCS.

## Network Agent fails to start with stealth mode NIC

### IP address removed from Linux configuration file

Network Agent can work with a stealth mode NIC only if the interface retains its old IP address in the Linux system configuration file. If you have bound Network Agent to a network interface card configured for stealth mode, and then removed the IP address of the NIC from the Linux configuration file (`/etc/sysconfig/network-scripts/ifcfg-adapter name`), Network Agent will not start.

An interface without an IP address will not appear in the list of adapters displayed in the installer or in Websense Manager and will be unavailable for use. To reconnect Network Agent to the NIC, restore the IP address in the configuration file.

### Stealth mode NIC selected for Websense communications in Solaris and Linux

Network interface cards configured for stealth mode in Solaris and Linux are displayed in the Websense installer as choices for Websense communications. If you have inadvertently selected a stealth mode NIC for communications, Network Agent will not start, and Websense services will not work.

To correct this problem, open the `websense.ini` file in `Websense/bin` and change the IP address to that of a NIC in normal mode. Start the Websense services.

## Windows 9x workstations are not being filtered as expected

If you are running DC Agent for user identification, your Windows 9x workstation machine names must not contain any spaces. This situation could prevent DC Agent from receiving a user name when an internet request is made from that workstation. Check the machine names of any Windows 9x workstations experiencing filtering problems and remove any spaces you find.

## I am using Logon Agent and some users are receiving the Websense Global policy

There may be a number of reasons why users are not being filtered as expected; however, if your network uses Logon Agent to identify users, and if some of those users are receiving the Websense Global policy instead of their usual user or group policies, a network problem may exist.

If the Logon Agent logon script fails to execute properly on a workstation, the Websense software cannot identify the user to apply the proper policy. The Global policy will be applied as a default.

The first step is to determine if the settings for the Windows Group Policy Objects (GPO) are being applied correctly to these workstations. If not, then this is a network connectivity problem and not a Websense configuration issue.

Proceed with the following network checks:

- ◆ Check the user machine's visibility to the domain controller from which the logon script is being run.
- ◆ Make sure that NetBIOS is enabled on the machine.
- ◆ Make sure the user profile is not blocking the execution of the logon script.

## Domain Controller Visibility

To determine if the domain controller is visible to the workstation:

- ◆ Attempt to map a drive on the client workstation to the domain controller's root shared drive. This is the drive from which the logon script is normally run, and on which LogonApp.exe resides.
- ◆ Run the following command from a Windows command prompt on the workstation that is not being identified:

```
net view /domain:<domain name>
```

If either of these tests fails, see your Windows operating system documentation for possible solutions. This is a network connectivity problem and not a Websense issue.

## NetBIOS

Make sure that NetBIOS for TCP/IP is enabled and that the TCP/IP NetBIOS Helper service is running on the client machine. If either of these is not running, the Websense logon script will not execute on the user machine.

The TCP/IP NetBIOS Helper service runs on Windows 2000, Windows XP, Windows Server 2003, and Windows NT. In Windows 98, TCP/IP NetBIOS is enabled by default.

If your network uses Active Directory, and if you have Windows 98 client machines, go to the Microsoft website for assistance: <http://technet.microsoft.com/en-us/windowsserver/2000/default.aspx>.

## User Profile Issues

If the user profile on the local workstation is corrupt, it can prevent the Websense logon script (as well as the Windows GPO settings) from running. To eliminate this as a cause:

1. Log on to the workstation as a local administrator.
2. Delete the following directory that contains the user profile:  
`C:\Documents & Settings\<user name>`
3. Restart the machine.
4. Log on as the normal user.  
The user profile will be created automatically.
5. Check to make sure the user is being filtered as expected.

## Websense splash screen is displayed, but installer does not launch on Windows 2000

This problem is a software issue with the installation machine which prevents it from displaying the Java-based Websense installer interface. This problem also prevents Websense Manager from launching on this machine.

There are two possible solutions for this problem.

- ◆ **Install DirectX on the installation machine.** DirectX is a Windows suite of application programming interfaces (APIs) that developers use to write applications for the Windows operating system. The Java-based Websense installer uses these APIs to display its interface, as does Websense Manager. If DirectX is not present, neither the Websense installer interface nor the Websense Manager interface can be displayed.
- ◆ **Run the installer in console mode.** You can configure `Setup.exe` to start in a Windows command prompt, which will allow you to install Websense software in the console mode.

To install Websense software in console mode:

1. Open the `launch.ini` file using a text editor.  
This file is located on the same level as `Setup.exe` in the folder where you unzipped your Websense installer.
2. Add the following line to the file:  
`ARGS=-console -is:javaconsole`
3. Save the file and exit.
4. Double-click `Setup.exe` or run the application from the command line.  
The installer starts in the Windows command prompt.
5. Follow the onscreen instructions to install Websense software.

**Note**

The installation sequence for the console mode is identical to that of the GUI mode.

---

6. Install Websense Manager on a Solaris machine or a Windows machine capable of displaying the Java interface.

## Network Agent cannot communicate with Filtering Service after it has been reinstalled

When Filtering Service has been uninstalled and reinstalled, Network Agent does not automatically update the internal identifier (UID) for the Filtering Service. After the new installation of Filtering Service is complete, Websense Manager still attempts to query Filtering Service using the old UID, which no longer exists.

To re-establish connection to the Filtering Service:

1. Open Websense Manager.  
An error message is displayed stating **Network Agent <IP address> is unable to connect with Filtering Service.**
2. Clear the message and select **Server > Settings.**  
The same error message is displayed.
3. Clear the message again and select **Network Agent** from the **Settings Selections** list.
4. Click **Local Settings.**
5. Select the IP address listed above the NIC for the Network Agent.
6. Click **Edit Selection.**  
The **Filtering Service Connection** dialog box appears.
7. Select the IP address of the Filtering Service machine from the **Server IP Address** drop-down list.
8. Click **Finish.**
9. Click **OK** in the **Local Settings** dialog box.
10. Click **OK** in the **Settings** dialog box to save the changes.

## Websense dictionary does not load in FireWall-1

The Get Dictionary process occurs between the FireWall-1 Management Module and Filtering Service. If the Management Module is not installed on the same machine as the FireWall Module, you may need to configure FireWall-1 to allow communication between the two machines running the Management Module and Filtering Service.

There are several reasons why the dictionary might not load within FireWall-1, as described below.



## Port mismatch

If the **FW1\_ufp** Service defined in FireWall-1 uses a different port than the Filtering Service filtering port (default 18182), Websense software cannot communicate with FireWall-1. As a result, FireWall-1 cannot retrieve the Websense dictionary entries.

Check for mismatched port entries in the following places:

- ◆ Check the **FW1\_ufp** Service definition in FireWall-1.
  1. From the FireWall-1 client, choose **Manage > Services**.
  2. Select **FW1\_ufp** from the list of services.
  3. Click **Edit**.

The **TCP Services Properties** dialog box appears.
  4. Make sure the port number displayed is the same as the number you defined for the filtering port when you installed the Filtering Service.
- ◆ Open the `ufp.conf` file (found in `websense\bin\FW1`) with a text editor. Check the port value to make sure it matches the port setting for the **FW1\_ufp** Service in FireWall-1.
- ◆ In FireWall-1, the filtering port specified in the `fwopsec.conf` file must match the port number set for the **FW1\_ufp** Service (and the port defined in the Websense `ufp.conf` file).



### Note

If the FireWall-1 module and the Management module are installed on separate machines, both contain an `fwopsec.conf` file. You must reconcile the filtering port number in each of these files as well.

---

## Communication mismatch

If the Websense dictionary does not load, check your communications settings. The method of communication selected in the OPSEC Application Object must be consistent with that defined in the `ufp.conf` file (Secure Internal Communication (SIC) or clear communication).

For example, if you have selected *early version compatibility* mode in the **OPSEC Application Object** dialog box (see [Early Versions Compatibility Mode, page 246](#)), the first line in the `ufp.conf` file must be:

```
ufp_server port 18182
```

If you have selected SIC, the first line in the `ufp.conf` file must be:

```
ufp_server auth_port 18182
```

## Policy properties

Although it is enabled by default, some environments need to disable the **Accept Outgoing Packet Originating from Gateway** setting in the FireWall-1 policy properties. Since the firewall cannot send any traffic in this environment, it cannot request the dictionary. To enable the dictionary request, add the following rule to the Rule Base anywhere before the “cleanup rule”:

**Source:** FireWall-1 workstation object  
**Destination:** Any or the Filtering Service workstation object  
**Service:** FW1\_ufp  
**Action:** Accept  
**Track:** Long (or any desired setting)  
**Install On:** SRC (*Required*)  
**Time:** Any

## SIC trust configuration in FireWall-1 NG

When you click **Get Dictionary** in the **Match** tab of the **URI Definition** dialog box, FireWall-1 NG (Feature Pack 1 or later) contacts the Filtering Service via SIC trust to retrieve a list of categories for use in FireWall-1 rules. If the SIC trust was not configured correctly, this contact fails and no categories can be retrieved.

To set up the SIC trust, follow the procedures in [Establishing Secure Internal Communication \(SIC\), page 234](#).

If you established the SIC trust, but still cannot get the dictionary, use the following steps to re-establish the trust.

1. Go to the FireWall-1 machine.
2. Choose **Manage > Servers and OPSEC Applications** to open the **Servers and OPSEC Applications** dialog box.

3. Select the Websense UFP Server object in the list, and then click **Edit** to display the **OPSEC Application Properties** dialog box.
4. Click **Communication** to display the **Communications** dialog box.
5. Click **Reset** to remove the SIC trust initialized previously, then click **Yes** in the confirmation dialog box that appears.
6. Click **Close** in the **Communications** dialog box.
7. Click **OK** to close the **OPSEC Application Properties** dialog box.
8. Click **Close** to close the **Servers and OPSEC Applications** dialog box.
9. Select **Policy > Install** to install the policy on the firewall.
10. Create the SIC trust again by following the procedures under [Establishing Secure Internal Communication \(SIC\)](#), page 234. (Do not create a new OPSEC Application Object for the Websense UFP Server; edit the one that already exists.)

## I configured FireWall-1 NG with AI for Enhanced UFP performance, and internet requests are not being filtered

Users who have configured FireWall-1 NG with AI for Enhanced UFP performance may not be able to filter internet requests. This is a Check Point licensing issue and not a configuration problem. A license from an older version of NG will not work with the newer version of NG with AI. Contact Check Point to update your license for your version of FireWall-1 NG with AI.

## FTP requests are not being blocked by protocol

Websense filtering software cannot block FTP requests when FireWall-1 is configured to act as a proxy. The FTP request is sent to FireWall-1 as **ftp://**. FireWall-1 then sends the packet to the Websense software with an **http://** header. The Websense software performs a lookup against HTTP categories instead of performing a protocol lookup, and the FTP request is permitted.

The best solution is to use the capability of FireWall-1 to block the FTP protocol.

1. In FireWall-1, create a rule that blocks on the FTP service.
2. Place this rule above the Websense rule.
3. Save the policy.

Users will receive the FireWall-1 block page instead of the Websense block page.



**Note**

In this case, it is not necessary to set the FTP protocol to be blocked in Websense Manager.

---

## Users filtered by remote filtering do not receive block pages

If users with the Remote Filtering Client on their workstations are being filtered properly, but are not receiving Websense block pages, try the following:

- ◆ If there is a firewall between the Websense Filtering Service machine and the Remote Filtering Server machine, check that it has been properly configured, as described in *Enabling communication between Remote Filtering Server and Filtering Service*, page 210:

- Make sure the **Block Page port** (by default, 15871) has been opened on the firewall. This allows Filtering Service to send block pages to remote users.

See the documentation for your firewall product if you need information about how to configure your firewall.

- ◆ Make sure Remote Filtering Client is not installed on the Remote Filtering Server machine. An instance of Remote Filtering Client running on the Remote Filtering Server machine eventually uses all available connections to the server. When the connections are not available, remote workstations cannot connect to the Remote Filtering Server and are not filtered. Uninstall the Remote Filtering Client from the Remote Filtering Server machine.

## Remote filtering is not working

If you installed the remote filtering components, but the user workstations on which you installed the Remote Filtering Client are not being filtered properly, you may have one or more of the following problems:

- ◆ You do not have the correct subscription key to enable the remote filtering service.
- ◆ Remote Filtering Server is not running.

- ◆ Remote Filtering Server and Filtering Service are installed on the same machine.
- ◆ Firewalls located between Remote Filtering Server and the Filtering Service have not been correctly configured.
- ◆ The external network firewall and any additional firewalls located between the Remote Filtering Server machine and the remote workstations have not been correctly configured.
- ◆ Network Agent is filtering responses to remote filtering requests.
- ◆ Other connection problems.
- ◆ DHCP is enabled for the Remote Filtering Server machine.
- ◆ The Remote Filtering Server machine is running Windows Server 2003, but Service Pack 1 is not installed.
- ◆ Parameters for communication between Remote Filtering Server and Remote Filtering Clients are not properly configured:
  - IP addresses for internal and external communication are not properly configured.
  - Ports for internal and external communication are not properly configured.
- ◆ Pass phrases entered for Remote Filtering Server and Remote Filtering Clients do not match.
- ◆ If a load balancer is in use, it is not forwarding packets to the Remote Filtering Server.

## Troubleshooting Procedure for remote filtering

Follow these procedures to determine the cause of the problem:

1. Check that your subscription key includes remote filtering.

The remote filtering service is available as an optional add-on. Check that your Websense subscription key includes the remote filtering service.
2. Check that Remote Filtering Server is running.
  - Windows: Use the Windows Services Control Panel to check that **Websense Remote Filtering Service** is running.
  - Linux and Solaris:
    - a. Go to the `/opt/Websense` directory.
    - b. From a command prompt, run `./WebsenseAdmin status`

- c. The Remote Filtering Server service should be running. If not, run `./WebsenseAdmin start`

3. Make sure Remote Filtering Server is *not* installed on the same machine as Filtering Service.

Installing these components on the same machine will cause a serious drain on resources on the machine. Filtering will become very slow, and may eventually fail and allow all requests.

4. Check that any firewalls located between Websense Filtering Service and Remote Filtering Server are correctly configured.

If there are one or more firewalls between the Filtering Service machine and the Remote Filtering Server machine, check that they have been properly configured, as described in *Enabling communication between Remote Filtering Server and Filtering Service*, page 210.

- Make sure the Filtering Service's **Filter port** (by default, 15868) has been opened on all firewalls between the Filtering Service and Remote Filtering Server. If this port is not open, Filtering Service cannot accept connections from the Remote Filtering Server.
  - Make sure that the **Block Page port** (by default, 15871) has been opened on all firewalls between the Filtering Service and Remote Filtering Server. If this port is not open, Filtering Service cannot send block pages to remote users.
5. Check that the external network firewall and any additional firewalls located between the Remote Filtering Server machine and the remote workstations have been properly configured, as described in *Enabling communication between Remote Filtering Server and Remote User Workstations*, page 209.
    - The Remote Filtering Server's **External Communication Port** on these firewalls must be able to accept connections from Remote Filtering Clients on workstations located outside the network firewall. By default, this is port 80, unless it was changed during installation of the Remote Filtering Server.
    - Access to the Remote Filtering Server's **Internal Communication Port** must be blocked from workstations located outside the network firewall. By default, this is port 8800, unless it was changed during installation of the Remote Filtering Server.

6. Make sure Network Agent is *not* filtering responses to remote filtering requests.

Check that Network Agent is *not* monitoring the machine on which Remote Filtering Server is installed:

- a. Open Websense Manager and connect to the Policy Server.
- b. Select **Server > Settings**.
- c. The **Settings** dialog box appears.
- d. In the **Settings** pane, click **Global Settings** under **Network Agent**.
- e. In the **Internal Network Definition** section of the window, check that the IP address for the machine running Remote Filtering Server is *not* included.
  - If the server's IP address is listed individually, select the address from the list and click **Delete**.
  - If the server's IP address is in a range, delete the range and add two ranges around that IP address.
- f. When you are finished, click **OK** at the bottom of the screen to save your changes.

See the Network Agent chapter in the *Administrator's Guide* for Websense Enterprise/Web Security Suite for more information about configuring Network Agent's global settings.

7. Check that connections are working properly.
  - Check that the remote workstations on which Remote Filtering Client has been installed are able to communicate with the Remote Filtering Server machine. The ping command can be used to verify this connection.
  - Check that the Remote Filtering Server machine is communicating properly with the network. Try to ping the Filtering Service machine and other machines on the local network.
8. Check the `RFSErrors.log` on the Remote Filtering Server machine.
  - a. Open the `RFSErrors.log` in a text editor. The default location of the `RFSErrors.log` file is:
    - Windows: `\Program Files\Websense\bin`
    - Linux and Solaris: `/opt/Websense/bin`
  - b. Check for error 64. This error might indicate that DHCP is enabled for the machine running the Remote Filtering Server.

- Acquire a static IP address and disable DHCP on this machine.
- c. Check for error 121. This error occurs in a Windows Server 2003 environment, and might indicate that Service Pack 1 is not installed. This service pack is required to run Remote Filtering Server.
  - Download and install the service pack from the Microsoft website.
- 9. Check that communications are properly configured for the Remote Filtering Server and the Remote Filtering Clients.

Remote Filtering Clients must be able to connect to the Remote Filtering Server from both inside and outside the internet gateway or network firewall. The correct communication information—IP addresses and port numbers for internal and external communications—must be entered during installation. See *Remote Filtering Server*, page 124 (Windows) or *Remote Filtering Server*, page 158 (Solaris and Linux) for more information.

- a. On the Remote Filtering Server machine, open the `securewispproxy.ini` file in a text editor. The default location of this file is:
  - Windows: `\Program Files\WebSense\bin`
  - Linux and Solaris: `/opt/WebSense/bin`
- b. Under `Proxy Server` parameters, make note of these settings:
  - **ProxyIP:** Must match the IP address of the network interface card (NIC) on the Remote Filtering Server machine that is used for internal communications.
  - **ProxyPort:** The port on the Remote Filtering Server machine used for external communications. The default is 80.
  - **ProxyPublicAddress:** The IP address or host name used for external access to the Remote Filtering Server machine from outside the external network firewall or internet gateway.
- c. Under `HeartBeat Server Parameters`, make note of the **HeartBeatPort** setting. This is the Internal Communication Port on the Remote Filtering Server machine, used for communication with Remote Filtering Client machines that have been moved inside the external network firewall. The default setting is 8800.
- d. Open a command prompt and run an IP configuration command on the Remote Filtering Server machine to get the IP addresses for each network interface card (NIC) in that machine:
  - Windows: `ipconfig`



- Linux and Solaris: `ifconfig -a`
  - e. Check that these IP address values match the Proxy Server parameters found in the `securewispproxy.ini` file.
  - f. The values need to be checked on the Remote Filtering Client machines. Contact Websense Technical Support for assistance. The technician will need the information gathered in the previous steps to verify that communications are properly configured.
10. Check that the pass phrases match.

The pass phrase for Remote Filtering Server and the Remote Filtering Clients must match. Checking to see if they match requires access to configuration and registry files. Incorrect changes to these files can interfere with machine operation. Contact Websense Technical Support for assistance.

If the pass phrase used for all Remote Filtering Clients does not match the pass phrase configured for the Remote Filtering Server:

- a. Reinstall the Remote Filtering Server and enter the proper pass phrase when prompted.
- b. Reinstall the Remote Filtering Clients, using the same pass phrase.

If Websense Client Policy Manager (CPM) is installed, or will be installed in the future, note the following:

- If Websense Client Policy Manager (CPM) is already installed in your network, you must enter the same pass phrase used when installing CPM.
- If you install CPM in your network in the future, you must use the same pass phrase you used to install the remote filtering components.

11. Ensure that the load balancer is forwarding packets to the Remote Filtering Server.

If you are using a load balancer, ensure that it is forwarding packets to the Remote Filtering Server. See your load balancing appliance or software documentation for configuration information.



## APPENDIX C | Technical Support

Websense, Inc., is committed to providing excellent service worldwide. Our goal is to provide professional assistance in the use of our software wherever you are located.

### Online Help

---

Select the **Help** option within the program to display detailed information about using the product.



#### Important

Default Microsoft Internet Explorer settings may block operation of the Help system. If a security alert appears, select **Allow Blocked Content** to display Help.

If your organization's security standards permit, you can permanently disable the warning message on the Advanced tab of the **Tools > Internet Options** interface. (Check **Allow active content to run in files on My Computer** under Security options.)

---

### Technical Support

---

Technical information about Websense software and services is available 24 hours a day at:

[www.websense.com/support/](http://www.websense.com/support/)

- ◆ the latest release information
- ◆ the searchable Websense Knowledge Base
- ◆ Support Forums
- ◆ Support Webinars

- ◆ show-me tutorials
- ◆ product documents
- ◆ answers to frequently asked questions
- ◆ Top Customer Issues
- ◆ in-depth technical papers

For additional questions, click the **Contact Support** tab at the top of the page.

If your issue is urgent, please call one of the offices listed below. You will be routed to the first available technician, who will gladly assist you.

For less urgent cases, use our online **Support Request Portal** at [ask.websense.com](http://ask.websense.com).

For faster phone response, please use your **Support Account ID**, which you can find in the Profile section at [MyWebsense](#).

Location	Contact information
North America	+1-858-458-2940
France	Contact your Websense Reseller. If you cannot locate your Reseller: +33 (0) 1 5732 3227
Germany	Contact your Websense Reseller. If you cannot locate your Reseller: +49 (0) 69 517 09347
UK	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Rest of Europe	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Middle East	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Africa	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Australia/NZ	Contact your Websense Reseller. If you cannot locate your Reseller: +61 (0) 2 9414 0033

<b>Location</b>	<b>Contact information</b>
Asia	Contact your Websense Reseller. If you cannot locate your Reseller: +86 (10) 5884 4200
Latin America and Caribbean	+1-858-458-2940

For telephone requests, please have ready:

- ◆ Websense subscription key
- ◆ Access to the Websense management console.
- ◆ Access to the machine running reporting tools and the database server (Microsoft SQL Server or MSDE)
- ◆ Familiarity with your network's architecture, or access to a specialist



# Index

## A

- activation key, 237
- Active Directory, 27
  - running logon script from, 201–202
- adding components
  - Linux, 170–172
  - Solaris, 170–172
  - Windows, 164–169
- Address Resolution Protocol (ARP), 253
- Apache HTTP Server
  - installing, 83, 115
- authentication
  - directory services, 27–30
  - User Service, 16
  - with RADIUS Agent, 118, 151

## B

- Bandwidth Optimizer, 9, 12, 76, 108, 147
- block messages
  - for protocols, 195–196
- block page port, 129, 162, 210
- block page URL, 194–195
- BrandWatcher, 208
- browser
  - path to, 146
  - proxy-based connections for, 31
- bytes transferred, 9

## C

- caching
  - no caching, 220
  - one request, 221
  - strategy for, 219
  - two request, 221
  - UFP Server caching, 221

- Citrix server users, filtering, 30
- clear communication, 242–245
- communicating with Websense Enterprise, 217
- components
  - adding, 163–172
  - removing, 173–178
  - repairing, 178–183
- config.xml
  - incompatibility of with previous versions, 35
  - repairing the Policy Server, 184
- config.xml file, 36
- Converting Stand-Alone Edition to Integrated system, 66
- customer support, 275
- customer support, *See* technical support

## D

- database download, *See* Master Database download
- DC Agent
  - defined, 9
  - deployment of, 19
  - installing separately
    - Windows, 112–114
  - on Linux
    - directory service support, 29
    - required privileges, 103
    - required privileges for, 79
- Default Web Site, 85, 116
- deploying Remote Filtering Client
  - third party tools for, 53
- deployment
  - component requirements, 15–23
  - directory services, 27–30
  - distributed, 25–26

- network requirements, 24–30
  - simple, 24–25
  - task list, 12
- dictionary
  - fails to load, 264–267
  - in FireWall-1 NG, NG with AI, and NGX, 227, 244
  - policy properties in FireWall-1, 266
- directory path for installation
  - Solaris and Linux, 98
  - Windows, 89
- directory services
  - supported types, 27–30
- DirectX requirement, 263
- DNS server, 194
- documentation
  - document conventions, 8
  - product guides and applicability, 7
  - Websense documentation website, 8
- domain administrator privileges, 79, 103
- domain controller
  - testing for visibility from, 261

**E**

- eDirectory Agent
  - defined, 9
  - deployment of, 20
  - installing separately
    - Linux, 153–155
    - Solaris, 153–155
    - Windows, 120–122
- eimserver.ini file, 36
  - identifying Filtering Service for block page URL, 195
- Enhanced UFP Performance, 245
- error messages
  - location of, 257
- evaluation key
  - website for downloading, 83, 95

**F**

- FailClose parameter
  - remote filtering, 210

- FailCloseTimeout parameter for remote filtering, 210
- files
  - backups of when upgrading, 36
- filter port, 129, 161
- Filtering Service
  - defined, 8
  - deployment of, 15
  - identifying for block page URL, 194–195
  - machine identification, 110, 129, 150, 161
  - multiple installations of, 25
  - port number, 83, 95
- FireWall-1
  - and client workstations, 217
  - distributed environments, 217
  - integrating with, 215–216
- FireWall-1 NG
  - clear communication, 242–245
  - configuration tasks, 223
  - creating OPSEC application objects, 224–228
  - creating resource objects, 228–230
  - defining rules for, 231–233
  - Secure Internal Communication (SIC) with, 234–242
- FireWall-1 NG with AI
  - clear communication, 242–245
  - configuration tasks, 223
  - configuring Enhanced UFP Performance, 245–250
  - creating OPSEC application objects, 224–228
  - creating resource objects, 228–230
  - defining rules for, 231–233
  - Secure Internal Communication (SIC) with, 234–242
- FireWall-1 NGX
  - clear communication, 242–245
  - configuration tasks, 223
  - configuring Enhanced UFP Performance, 245–250
  - creating OPSEC application objects, 224–228
  - creating resource objects, 228–230



defining rules for, 231–233  
 Secure Internal Communication (SIC)  
 with, 234–242

## G

Global Websense policy application, 261

## I

IIS Web Server

detecting, 83, 115

IM Attachment Manager, 9, 12, 76, 108, 147

installation

Apache HTTP Server, 83, 115

console mode in Windows, 263

Custom option, 76

DC Agent

Windows, 112–114

detecting IIS Web Server, 83, 115

eDirectory Agent

Linux, 153–155

Solaris, 153–155

Windows, 120–122

Filtering Service port, 83, 95

Logon Agent, 122–124

Linux, 155–158

Solaris, 155–158

Manager

Linux, 145–147

Solaris, 145–147

Windows, 106–107

Network Agent

Linux, 147–151

Solaris, 147–151

Windows, 108–112

Policy Server port, 83, 95

RADIUS Agent

Linux, 151–153

Solaris, 151–153

Windows, 118–120

Real-Time Analyzer, 114–118

Remote Filtering Client, 132–143

Remote Filtering Client Pack, 131–132

Remote Filtering Server, 124–130

Linux, 158–163

Solaris, 158–163

Windows, 124–130

Websense Enterprise

Linux, 91–100

separate Windows machine, 78–90

Solaris, 91–100

Websense Web Security Suite

Linux, 91–100

separate Windows machine, 78–90

Solaris, 91–100

Windows installer does not launch, 262

internet access problems, 258–259

IP addresses

changing for installed components, 72

defining ranges for Network Agent, 17, 108

disabling for stealth mode, 252

multiple network interface cards, 82

requirements for Websense

communication, 94

stealth mode and, 251

transparent identification for, 30

User Service requirements for, 16

## L

Language Pack, 36, 74

starting manually, 256

languages, 73

Language Pack, 36

locales, 16

launch.ini file, 263

LDAP directory service, 28

Linux

adding components on, 170–172

error messages, 257

removing components on, 176–178

repairing components on, 181–183

starting and stopping Websense

services, 188

upgrading Websense Enterprise on, 45–49

upgrading Websense Web Security Suite

on, 45–49

Websense Enterprise installation on, 91–100

Websense Web Security Suite installation

on, 91–100

- load balancing, 25
- locales, 16
- LocalLogSize parameter for remote filtering, 212
- logging
  - for Remote Filtering Client, 212
- Logon Agent
  - defined, 9
  - deployment of, 20
  - failure to identify users, 261–262
  - installing separately
    - Linux, 155–158
    - Solaris, 155–158
    - Windows, 122–124
- logon script
  - domain controller visibility issues, 261
  - enabling NetBIOS for, 262
  - user profile issues, 262
- LogonApp.exe
  - configuring to run
    - Active Directory, 201–202
    - Windows NTLM, 203–??
  - location of, 197
  - script for, 198–200

**M**

- MAC address, 253
- Manager, *See* Websense Manager
- manual authentication, 29
- Master Database
  - description of, 10
  - reloading when repairing Policy Server, 184
- Master Database download
  - and virus scanners, 259
  - during installation
    - Solaris and Linux, 95, 99
    - Windows, 89–90
  - during upgrade
    - Solaris and Linux, 48
    - Windows, 42–44
  - error message location, 257
  - failure of, 257–259
  - from Websense Manager, 190–194

- performing, 190–194
- Messenger Service, 196
- modifying an installation, 163–183

## N

- NetBIOS, 19
  - enabling for logon script, 262
- Network Agent
  - bandwidth optimizer, 76, 108, 147
  - capture interface, 86, 96, 110, 149, 167, 171
  - defined, 8
  - deployment of, 16
  - feedback on protocol usage, 86, 96
  - in switched environments, 17
  - installing separately
    - Linux, 147–151
    - Solaris, 147–151
    - Windows, 108–112
  - instant messaging attachment manager, 76, 108, 147
  - network interface card, 204
  - on firewall machine, 110, 149
  - protocol management, 108, 147
  - stealth mode NIC, 251–253
- network interface cards (NIC)
  - configuring for stealth mode
    - Solaris or Linux, 253
    - Windows, 252
  - installation tips, 77
  - selecting for Network Agent, 86, 96, 110, 167, 171
- no caching, 220
- non-English language versions, 73
- Novell Directory Service/eDirectory Agent, 28
- Novell Directory Services/eDirectory Agent, 28

**O**

- one request caching, 221
- OPSEC application objects
  - creating, 224–228
- opsec\_pull\_cert command, 238

**P**

- pass phrase for remote filtering, 127, 160
- password
  - forgotten, 257
  - Policy Server setting, 192
  - proxy server/firewall setting, 193
- Policy Server
  - defined, 8
  - deployment of, 15
  - failure to install, 259
  - machine identification, 109, 115
  - port number, 83, 95
  - repairing, 183–184
- port numbers
  - errors caused by mismatch, 265
  - Filtering Service, 110, 129, 150, 161
  - FireWall-1 messages, 215
  - Policy Server, 109, 115
- protocol block messages, 195–196
- Protocol Management, 9, 11, 76, 108, 147
- proxy server
  - settings for Master Database download, 193

**Q**

- QuickUFP, 245
- quotas, 11

**R**

- RADIUS Agent
  - defined, 9
  - deployment of, 21
  - installing separately
    - Linux, 151–153
    - Solaris, 151–153
    - Windows, 118–120
- Real-Time Analyzer (RTA)
  - defined, 9
  - deployment of, 18
  - installing separately, 114–118
  - launching, 90, 118, 169
  - supported web servers for, 83, 115
- Remote Filtering Client
  - block pages, receiving, 268

- defined, 10
- deployment of, 22
- installing
  - manually, 133
  - with third-party tools, 138
- local log, 212
- repairing an installation, 143
- setting to fail closed, 210
- troubleshooting, 268
- uninstalling, 143
- upgrading, 50
  - manually, 51
  - with third-party tools, 53
- Remote Filtering Client Pack
  - defined, 102
  - installing, 131–132
  - upgrading, 50
- Remote Filtering Server
  - DCHP incompatibility, 159
  - defined, 9
  - deployment of, 22
  - DHCP incompatibility, 125
  - External Communication Port, 127, 136, 139, 160
  - firewall configuration for, 209–210
  - installing
    - Linux, 158–163
    - Solaris, 158–163
    - Windows, 124–130
  - Internal Communication Port, 127, 137, 140, 160
  - pass phrase, 127, 160
  - troubleshooting, 268
  - upgrading, 50
- removing components
  - Linux, 176–178
  - Solaris, 176–178
  - Windows, 173–176
- repairing components
  - Linux, 181–183
  - Solaris, 181–183
  - Windows, 178–181
- Reporting Tools
  - deployment of components, 23

- installing, 76
- supported version, 37
- upgrading, 37
- Resource Objects
  - creating
    - NG, NG with AI, NGX, 228–230
  - updating, 71
- rules, defining
  - NG, NG with AI, NGX, 231–233

**S**

- Samba client, 98
- Secure Internal Communication (SIC)
  - OPSEC application object
    - creating, 234–237
    - updating, 239–242
  - prerequisites, 234
  - troubleshooting the SIC trust, 266–267
  - Websense configuration for, 237–239
- securewispproxy.ini file, 210, 212
- setup
  - block page URL, 194–195
  - Master Database download, 190–194
  - subscription key, 190–194
- SiteWatcher, 208
- Solaris
  - adding components on, 170–172
  - error messages, 257
  - removing components on, 176–178
  - repairing components on, 181–183
  - starting and stopping Websense services, 188
  - upgrading Websense Enterprise on, 45–49
  - upgrading Websense Web Security Suite on, 45–49
  - Websense Enterprise installation, 91–100
  - Websense Web Security Suite installation, 91–100
- Stand-Alone Edition
  - converting to integrated system, 54–70
- stealth mode, 94
  - configuring
    - Solaris or Linux, 253
    - Windows, 252

- definition of, 251
- problems with NIC, 260
- using with Network Agent, 251
- subscription key
  - dialog box, 83
  - entering, 190–194
  - Master Database download during installation with, 83, 95
  - verification and troubleshooting of, 257
- Sun Java System Directory Server, 28
- switched environments, 17
- system requirements, 24, 30
  - FireWall-1 versions supported, 31
  - workstations, 31

## T

- technical support, 275
- ThreatWatcher, 208
- Traffic Visibility Tool, 204
- transparent identification, 28, 29
- two request caching, 221

## U

- UFP Server
  - caching, 221
  - stopping, 186
- ufp.conf file, 239
- upgrading
  - distributed component, 36
  - from Stand-Alone Edition to integrated system, 54–70
    - all Websense filtering components on same machine, 55
    - move some Websense filtering components to other machines, 55
  - general information, 36–38
  - manually restarting services, 37
  - migrating to a newer FireWall-1 version, 37, 71, 185
  - non-English language versions, 36
  - on Linux, 45–49
  - on Solaris, 45–49
  - on Windows, 38–45
  - Remote Filtering Client, 50

- Remote Filtering Server, 50
- Resource Objects, updating, 71
- transferring data to fresh install, 35–36
- versions supported, 34
- Websense components on Windows, 38–44
- Usage Monitor
  - defined, 9
  - deployment of, 18
- user identification, 27–30
- user profile issues with logon script, 262
- User Service
  - defined, 8
  - deployment of, 16
  - required privileges, 79, 103
- V**
- virus scanners, 259
- W**
- Web Protection Services
  - BrandWatcher, 208
  - SiteWatcher, 208
  - ThreatWatcher, 208
- Websense Enterprise
  - communicating with FireWall-1, 217
  - component deployment, 15–23
  - component overview, 8–11
  - components
    - adding, 163–172
    - removing, 173–178
  - converting Stand-Alone Edition to integrated system, 54–70
  - deployment
    - distributed, 25–26
    - installed on same machine as FireWall-1, 27
    - simple, 24–25
  - functional overview, 11
  - initial configuration, 189
  - installation on
    - Linux, 91–100
    - Solaris, 91–100
    - Windows, 78–90
  - installing on
    - FireWall-1 machine, 75
    - selecting a NIC for communication, 251
    - versions supported for upgrade, 34
- Websense Enterprise Explorer, 10
- Websense Enterprise Explorer for Unix, 10
- Websense Enterprise Reporter, 10
- Websense Manager
  - defined, 8
  - deployment of, 15
  - does not launch, 262
  - installing separately
    - Linux, 145–147
    - Solaris, 145–147
    - Windows, 106–107
  - launching, 191
- Websense Master Database, *See* Master Database
- Websense services
  - manually stopping, 185–186
  - starting and stopping
    - Linux, 188
    - Solaris, 188
    - Windows, 186–188
  - stopping before upgrading, 37
- Websense Web Security Suite
  - component deployment, 15–23
  - component overview, 8–11
  - components
    - adding, 163–172
    - removing, 173–178
  - converting Stand-Alone Edition to integrated system, 54–70
  - deployment
    - distributed, 25–26
    - simple, 24–25
  - functional overview, 11
  - initial configuration, 189
  - initial configuration of Web Protection Services, 208
  - installation on
    - Linux, 91–100
    - Solaris, 91–100
    - Windows, 78–90
  - installing on

- FireWall-1 machine, 75
- versions supported for upgrade, 34
- websense.ini file, 36
- Websense.log, 257
- Windows
  - Active Directory, 27, 29
  - adding components on, 164–169
  - error messages, 257
  - NTLM-based directories, 27, 29
  - removing components on, 173–176
  - starting and stopping Websense services, 37, 186–188
  - upgrading Websense components on, 38–44
  - upgrading Websense on, 38–45
  - Websense Enterprise installation, 78–90
  - Websense Web Security Suite
    - installation, 78–90
- Windows NTLM
  - running logon script from, 203–??
- Windows XP SP2 and protocol block messages, 196
- winpopup.exe, 196
- workstations, 31
- WSSEK.dat file, 137